QUANTUM

2025年6月10日

QUANTUM SECURITY MANAGEMENT

R82

管理ガイド

CHECK POINT™

Check Point Copyright Notice

©2024 - 2025Check Point Software Technologies Ltd.

All rights reserved.本製品および関連ドキュメントは著作権法によって保護されており、その使用、複写、逆コンパイルを制限するライセンス契約に基づいて配布されています。本製品または関連ドキュメントのいかなる部分も、チェック・ポイントの書面による事前承諾を得ない限り、いかなる形態や方法によっても複製することはできません。本マニュアルを製作するにあたっては細心の注意が払われていますが、チェック・ポイントはいかなる誤りまたは欠落に対しても一切責任を負いません。本マニュアルおよびその記述内容は、予告なく変更される場合があります。

権利の制限

米国政府による本製品の使用、複写、または開示は、DFARS(連邦国防調達規定)252.227-7013およびFAR(連邦調達規定)52.227-19の技術データおよびコンピュータソフトウェアに関する権利条項(c)(1)(ii)により制限されます。

商標

当社の商標の一覧は、Copyright page を参照してください。

関連する著作権およびサードパーティライセンスの一覧は、Third Party copyright notices を参照してください。

重要な情報



最新版ソフトウェア
最新版ソフトウェアには、機能や安定性の向上、セキュリティの拡張、新たな脅威や進化する攻撃に対処する最新の保護機能が備えられています。常に最新版をインストールすることをお勧めします。



認定資格
サードパーティによるCheck Pointの認定資格については、Check Point Certifications pageを参照してください。



Check Point R82
このリリースに関する詳細については、R82のhome pageを参照してください。



最新版ドキュメント(英語版)
最新版(document in a Web browser)を確認ください。
最新版のダウンロードはこちら: document in PDF format



ご意見/ご感想
チェック・ポイントは、わかりやすいマニュアルの作成に日々取り組んでいます。
Please help us by sending your comments。



特許に関する通知
Check Point Quantum Security Managementは、米国およびその他の国における以下の特許により保護されています。
このページは、35 U.S.C. § 287(a)に基づく通知を意図しています:
US7,647,492, US7,769,862, US7,797,566, US7,950,059, US8,051,187, US8,146,159, US8,161,188, US8,176,539, US8,200,818, US8,254,698, US8,406,233, US8,533,808, US8,615,655, US8,644,328, US8,726,008, US8,776,017, US8,843,993, US8,844,019, US8,850,576, US8,902,900, US8,948,193, US8,959,047, US9,137,204, US9,208,317, US9,210,128, US9,356,945, US9,483,583, US9,537,756, US9,569,265, US9,647,985, US9,672,189, US9,832,215, US9,935,903, US10,057,390, US10,382,493, US10,467,407, US10,567,395, US10,567,468, US10,645,074, US10,728,266, US10,728,274, US11,075,882, US11,165,820, US11,321,453, US11,323,426, US11,411,924, US11,606,375

改訂履歴

日付	説明
2025年5月28日	更新 *オンプレミスのSecurity Management Serverとセキュリティゲートウェイを Infinity Portalに接続する (537ページ)*
2025年4月27日	更新 *HTTPSインスペクション (541ページ)*
2025年4月6日	追加 *TLS接続のブロック (576ページ)*
2025年3月23日	追加 *ポリシーインサイト (396ページ)* 更新 *SAML認証ログインによる管理者アカウントの作成 (101ページ)*
2025年3月14日	章を更新 *アクセスコントロールポリシーのUserCheck (516ページ)*
2025年2月25日	更新 *ホットフィックスとバージョンアップの一元的な展開 (245ページ)*- 「制限事項」セクションにMaestroおよびElasticXLクラスタのセキュリティグループを追加
2025年2月6日	更新: ■ *SmartConsoleウィンドウ (36ページ)* ■ *SmartConsoleのツールバー (37ページ)*
2025 年 1 月 5 日	追加: ■ *SmartConsoleパッケージ (32ページ)* ■ *脅威の分析 (515ページ)* ■ *SmartConsoleの新機能のテスト (667ページ)* 更新: ■ *アクセス、カスタム、HTTPSインスペクションツール (44ページ)* ■ *SmartConsoleのキーボードショートカット (48ページ)* ■ *更新可能なオブジェクト (295ページ)* ■ *管理者アカウントの管理 (74ページ)* ■ *ユーザアカウントの管理 (136ページ)*
2025年1月1日	更新 *セキュリティゾーン (304ページ)*

日付	説明
2024年12月29日	更新: ■ *NATの背後にあるSecurity Management (477ページ)* ■ *HTTPSインスペクション (541ページ)*
2024年12月15日	更新 *HTTPSインスペクション (541ページ)*
2024年12月01日	更新 *SmartTasks (600ページ)*
2024年11月04日	更新 *Health Check Point Tool (276ページ)*
2024年10月21日	初版

目次

Quantum Security Managementについて ... *30*

セキュリティ管理設定のワークフロー ... *30*

SmartConsoleパッケージ ... *32*

SmartConsoleでSecurity Management Serverに接続する ... *33*

SmartConsoleを理解する ... *35*

SmartConsoleウィンドウ ... *36*

SmartConsoleのツールバー ... *37*

検索エンジン ... *41*

IP検索 ... *41*

一般的なIP検索 ... *41*

パケットサーチ ... *42*

ルールベース結果 ... *42*

アクセス、カスタム、HTTPSインスペクションツール ... *44*

セキュリティポリシー"アクセスコントロール"ビューの"アクセスツール" ... *44*

セキュリティポリシー「脅威対策」ビューの「カスタムポリシーツール」 ... *44*

セキュリティポリシーHTTPSインスペクションビューのHTTPSインスペクションツール ... *45*

共有ポリシー ... *46*

APIコマンドラインインタフェース ... *47*

SmartConsoleのキーボードショートカット ... *48*

SmartConsoleでのInfinity AI Copilotの使用 ... *50*

事前準備 ... *50*

Security Managementの計画 ... *52*

Security Management Serverのサイズ ... *52*

組織のトポロジの定義 ... *53*

組織のリソースを保護するためのアクセスルールの定義 ... *53*

アクセスポリシーの実施 ... *53*

Security Management Serverとセキュリティゲートウェイの設定 ... *54*

APIによるセキュリティ管理 ... *56*
API ... *56*
APIツール ... *57*
APIサーバの設定 ... *57*
セルフマネージドセキュリティゲートウェイ ... *60*
はじめに ... *60*
必要条件 ... *61*
制限事項 ... *62*
注 ... *63*
設定 ... *63*
ダイナミックレイヤーのリセット ... *69*
APIキー認証による管理者アカウントの作成 ... *71*
管理者アカウントの管理 ... *74*
管理者アカウントの作成 ... *74*
管理者アカウントの編集 ... *77*
管理者アカウントの削除 ... *77*
管理者のデフォルト有効期限 ... *78*
SmartConsole セッションタイムアウトの設定 ... *79*
管理者証明書の失効 ... *79*
管理者のログイン試行の制限 ... *80*
管理者アカウントのロック解除 ... *80*
複数の管理者 ... *80*
Check Pointのパスワード認証による管理者アカウントの作成 ... *81*
OSパスワード認証による管理者アカウントの作成 ... *84*
RADIUSサーバ認証による管理者アカウントの作成 ... *87*
TACACS サーバ認証による管理者アカウントの作成 ... *92*
SecurID認証による管理者アカウントの作成 ... *97*
SAML認証ログインによる管理者アカウントの作成 ... *101*
使用事例 ... *101*
SAML認証ログイン ... *102*

APIキー認証による管理者アカウントの作成 113
管理者への権限プロファイルの割り当て 116
権限プロファイルの変更と作成 116
カスタマイズされた権限の設定 118
アクセスコントロールレイヤーの権限の設定 120
アクセスコントロールと脅威対策のためのアクセス許可の設定 121
モニタ、ログ、イベント、レポートの権限の設定 122
信頼できるクライアントの定義 123
管理者向けセッションフロー 126
セッションの公開 126
SmartConsoleのセッションビューでの作業 127
プライベートセッションで行った変更の表示 128
非アクティブなセッションを持つ管理者からロックされたオブジェクトを引き継ぐ 128
複数のセッションで作業する管理者 129
セッションの承認サイクル(SmartWorkflow および Identity Provider) 132
使用事例 132
設定 132
チームワークのセッティング 135
ユーザアカウントの管理 136
ユーザアカウントの作成 136
既存ユーザの変更 139
ユーザの削除 139
ユーザグループの管理 140
ユーザのデフォルト有効期限設定の設定 141
ユーザの管理 142
新しいユーザテンプレートの作成 142
新規ユーザの作成 143
既存ユーザの編集 144
ユーザの削除 144
ユーザのデフォルト有効期限設定の設定 145

Check Pointのパスワード認証を使用したユーザアカウントの作成 146
OSパスワード認証によるユーザアカウントの作成 150
RADIUSサーバ認証によるユーザアカウントの作成 154
ユーザに対するRADIUS認証の設定 154
RADIUSサーバグループを使用したユーザアクセスの許可 160
TACACSサーバ認証によるユーザアカウントの作成 161
SecurID認証によるユーザアカウントの作成 168
アクセスロール 177
アクセスロールの追加 177
ユーザディレクトリ 179
ユーザディレクトリに関する考察 179
ユーザディレクトリの展開 180
ユーザディレクトリの有効化 181
LDAP用ユーザディレクトリスキーマ 181
スキーマチェック 182
OID専用属性 182
ユーザディレクトリスキーマ属性 182
ユーザ情報の効率的な取得 193
User-to-Groupメンバシップモードの設定 193
プロフィール属性 193
ユーザディレクトリサーバでのユーザ管理 204
複数のサーバへのユーザの分散 204
LDAP情報の管理 204
ユーザディレクトリのLDAPグループ 205
User Directoryサーバからの情報の取得 207
User Directoryのクエリの実行 207
複数のLDAPサーバへのクエリ 208
アカウントユニット 209
LDAPアカウント単位での作業 209
LDAPクエリパラメータの設定 214

LDAPサーバの変更 215
アカウントユニットとハイアベイラビリティ 215
ハイアベイラビリティ優先度の設定 216
証明書での認証 216
外部LDAPサーバ上のユーザの設定 218
Microsoft Active Directory 218
パフォーマンス 218
管理 218
実施 218
レジストリ設定の更新 219
制御の委任 219
Active Directoryスキーマの拡張 219
Active Directoryへの新しい属性の追加 220
Active Directory上のLDAPアカウントユニットに対するユーザまたはサービスアカウントのパスワードの更新 221
ゲートウェイの管理 222
SIC (Secure Internal Communication) 222
トラストの初期化 222
SICステータス 223
トラスト状態 223
SICのトラブルシューティング 224
Check Point内部認証局 (ICA) について 225
ICAクライアント 225
SIC証明書の管理 225
セキュリティゲートウェイの新規作成 227
ゲートウェイトポロジの手動更新 229
インタフェースの取得 API 230
セキュリティゲートウェイトポロジの動的な更新 231
動的アンチスプーフィング 231
ライセンスの管理 232

サーバとゲートウェイのライセンス管理 ... 233
SmartConsoleでのライセンスの表示 ... 235
VSXのライセンス情報の表示 ... 236
SmartConsoleでのライセンスのモニタ ... 237
ライセンスまたはクォータの変更 ... 239
セキュリティゲートウェイインジケータ ... 241
セキュリティゲートウェイへの推奨Takeのインストール ... 242
ホットフィックスとバージョンアップの一元的な展開 ... 245
はじめに ... 245
事前準備 ... 246
制限事項 ... 247
インストール ... 247
HotfixまたはJumbo Hotfix Accumulatorのアンインストール ... 251
セントラルデプロイメントによるクラスタのアップグレード方法 ... 252
NATed IPアドレスで管理サーバまたはログサーバにアクセスするセキュリティゲートウェイの設定 ... 253
セキュリティゲートウェイの暗黙ルールまたはカーネルテーブルの設定 ... 254
はじめに ... 254
設定ファイル ... 254
設定手順 ... 256
Management Serverの'user.def'ファイルの場所 ... 257
Management Server上の'implied_rules.def'ファイルの場所 ... 258
Management Server上の'table.def'ファイルの場所 ... 260
管理サーバ上の'crypt.def 'ファイルの場所 ... 262
Management Server上の「vpn_table.def」ファイルの場所 ... 264
管理サーバ上の「vpn_route.conf」ファイルの場所 ... 266
管理サーバ上の'communities.def'ファイルの場所 ... 268
管理サーバ上の'base.def'ファイルの場所 ... 270
Management Server上の'dhcp.def'ファイルの場所 ... 272
Management Serverの'gtp.def'ファイルの場所 ... 274

Health Check Point Tool ... 276
SmartConsoleのステータス ... 278
制限事項 ... 278
オブジェクトの管理 ... 279
オブジェクトのカテゴリ ... 280
オブジェクトを使ったアクション ... 281
オブジェクトタグ ... 283
オブジェクトへのタグの追加 ... 283
ネットワークオブジェクトの種類 ... 284
ネットワーク ... 284
ネットワークグループ ... 285
ネットワークオブジェクトのグループ化 ... 285
Check Pointホスト ... 286
ゲートウェイクラスタ ... 287
アドレス範囲 ... 288
ワイルドカードオブジェクト ... 289
ワイルドカードオブジェクトについて ... 289
IPv6 ... 293
ドメイン ... 294
更新可能なオブジェクト ... 295
更新可能オブジェクトについて ... 295
アクセスコントロールポリシーへの更新可能オブジェクトの追加 ... 295
カスタム脅威対策ポリシーへの更新可能オブジェクトの追加 ... 296
HTTPSインスペクションポリシーへの更新可能オブジェクトの追加 ... 297
更新可能オブジェクトのモニタリング ... 298
管理サーバによる更新可能オブジェクトの更新 ... 299
ダイナミックオブジェクト ... 301
一般的なデータセンターオブジェクト ... 302
制限事項 ... 303
セキュリティゾーン ... 304

セキュリティゾーンとNATルール使用時のルールベース実行処理のフロー ... 305
セキュリティゾーンの作成と割り当て ... 305
事前定義されたセキュリティゾーン ... 306
制限事項 ... 307
外部管理のゲートウェイとホスト ... 308
相互運用可能なデバイス ... 309
VoIPドメイン ... 310
論理サーバ ... 311
バランス方式 ... 311
OSE(Open Security Extension) デバイス ... 312
OSEデバイスインタフェースの定義 ... 312
OSデバイスプロパティウィンドウ- 一般タブ ... 313
なりすまし防止パラメータとOSデバイスのセットアップ(Cisco) ... 313
ポリシーの管理 ... **315**
ポリシーパッケージでの作業 ... 315
ルールログの表示 ... 322
ポリシーインストール履歴 ... 323
同時インストールポリシー ... 324
Accelerated Install Policy ... 325
アクセスコントロールポリシーの作成 ... **326**
統合アクセスコントロールポリシーの導入 ... 326
アクセスコントロールルールベースのカラム ... 327
送信元と送信先のカラム ... 328
ネットワークオブジェクトについての詳細 ... 328
VPNカラム ... 328
IPsec VPN ... 329
ネットワークへのモバイル・アクセス ... 329
VPNの詳細について ... 329
サービス＆アプリケーションカラム ... 330
サービスマッチング ... 330

アプリケーションマッチング ... 330
R77.30以下のセキュリティゲートウェイにおけるサービスとアプリケーション、およびアップグレード後について ... 333
コンテンツカラム ... 334
アクション ... 335
追跡カラム ... 337
追跡(トラッキング)の詳細について ... 337
アクセスコントロールポリシーのルールマッチング ... 338
マッチングの例では: ... 341
基本的なアクセスコントロールポリシーの作成 ... 343
基本ルール ... 343
使用例 - 基本的なアクセスコントロール ... 343
使用例 - 各部門のインラインレイヤー ... 345
セルのデフォルト値 ... 348
値 "None"を持つルールの実行 ... 348
R81以前のManagement Serverからのアップグレード ... 349
アプリケーションコントロールとURLフィルタリングのルールの作成 ... 350
URLカテゴリのブロック ... 356
オーダーレイヤーとインラインレイヤー ... 358
オーダレイヤーとインラインレイヤーの必要性 ... 358
インラインレイヤーにおけるルール実行の順序 ... 358
Ordered Layersにおけるルール実行の順序 ... 359
インラインレイヤーの作成 ... 360
Ordered Layerの作成 ... 361
アクセスコントロール機能の有効化 ... 363
ルールベースにおけるルールの種類 ... 364
アクセスコントロールレイヤーの管理者 ... 367
レイヤーの共有 ... 367
ルールベースのセクションによる視覚的分割 ... 368
ポリシーとレイヤーの管理 ... 368

アクセスコントロールルールのベストプラクティス ... 370
統一ルールベースの使用例 ... 372
セルフマネージドセキュリティゲートウェイ ... 384
はじめに ... 384
必要条件 ... 385
制限事項 ... 386
注 ... 387
設定 ... 387
ダイナミックレイヤーのリセット ... 393
アクセスコントロールポリシーのインストール ... 395
ポリシーインサイト ... 396
対応オブジェクト ... 396
事前準備 ... 396
ポリシーインサイトでの作業 ... 396
ポリシーインサイト ウィンドウのコンポーネント ... 397
セキュリティゲートウェイR77.30(およびそれ以下)と統合アクセスコントロールポリシー ... 399
ルールベースのヒットカウントの分析 ... 400
ヒット数の有効化または無効化 ... 400
ヒットカウントの表示 ... 401
IPスプーフィングの防止 ... 403
アンチスプーフィングオプション ... 406
NATポリシーの設定 ... 407
NATの使用 ... 407
はじめに ... 407
NATルールの種類 ... 408
NAT方式の種類 ... 409
SmartConsoleのNATルール ... 412
NATルール実施の順番 ... 414
自動NATルールの操作 ... 415
自動NATルールの例 ... 415

自動NATの設定 418
デプロイメント例 419
外部ネットワークへの自動Hide NAT 423
Manual NATルールの操作 425
手動NATルールの例 425
手動NATの設定 426
デプロイメント例 426
NAT46ルールの操作 431
メニュー 431
NAT46の既知の制限事項 433
NAT46の設定 433
NAT46トラフィックのログ 446
NAT64ルールの操作 447
メニュー 447
NAT64の既知の制限事項 448
NAT64変換フロー例 449
NAT64の設定 451
NAT64トラフィックのログ記録 467
高度なNAT設定 468
自動およびプロキシ ARP 468
NATとアンチスプーフィング 469
VPNトンネルのNATを無効にする 470
アドレスが重複する社内通信 471
ネットワーク設定例 471
コミュニケーション例 472
ルーティングの考慮事項 473
オブジェクトデータベースの設定 473
マルチキャストアクセスコントロール 475
NATの背後にあるSecurity Management 477
メニュー 477

Security Management Serverのコントロール接続用NATの設定 478
セキュリティゲートウェイの設定 478
IPプールNAT 480
メニュー 480
NATの優先順位 481
インタフェースごとのIPプール 482
IPプールアドレスを異なる宛先に再利用する 483
IPプール設定手順 485
ネットワークへのモバイル・アクセス 489
Check Pointのモバイルアクセスソリューション 489
クライアントベースとクライアントレス 489
モバイルアクセスクライアント 490
モバイルアクセスWebポータル 490
SSL Network Extender 490
ネットワークリソースへのモバイルアクセスの設定 491
モバイルアクセスワークフローの例 491
モバイルアクセスの展開例 492
モバイルアクセス設定ウィザードの使用 493
モバイル接続の許可 494
アプリケーションへのアクセスの定義 495
シングルサインオンの有効化 495
Citrixサーバへの接続 497
Citrixサーバを使用したサンプルデプロイメント 497
モバイルアクセス向けCitrixサービスの設定 498
コンプライアンスチェック 500
コンプライアンスポリシー ルール 500
コンプライアンスポリシーの作成 500
セキュリティゲートウェイのコンプライアンスの設定 501
Secure Workspace 502
Secure Workspace 503

モバイルアクセスについての詳細 504
サイト間VPN 505
サイト間VPNの導入例 505
VPNコミュニティ 505
VPNコミュニティの組合せ例 508
VPN接続の許可 508
VPNアクセスコントロールルールのサンプル 509
サイト間VPNについての詳細 509
リモート アクセス VPN 510
VPN接続モード 510
リモートアクセスVPNワークフローの例 510
リモートアクセスコミュニティのセキュリティゲートウェイの設定 512
リモートアクセスVPNについて 512
暗黙のルール 513
新しい脅威対策ポリシーの作成 514
脅威対策ポリシーのインストール 514
脅威の分析 515
アクセスコントロールポリシーのUserCheck 516
UserCheckの設定 518
Access Control Software BladesのUserCheckインタラクションオブジェクト 522
UserCheckインタラクションのアクションタイプ 522
アクセスコントロールのためのデフォルトのUserCheckインタラクションオブジェクト 523
アクセスコントロールのための新しいUserCheck相互作用オブジェクトの作成 523
プレーンテキストでEメール通知を送信 528
UserCheck ポータルのローカライズとカスタマイズ 530
外部ネットワークフィード 531
使用事例 531
モニタリング 534
トラブルシューティング 535

オンプレミスのSecurity Management ServerとセキュリティゲートウェイをInfinity Portalに接続する ... *537*
事前準備 ... *537*
トラブルシューティング ... *540*
HTTPSインスペクション ... *541*
HTTPS接続の遮断 ... *542*
アウトバウンド HTTPSインスペクション ... *542*
インバウンド HTTPSインスペクション ... *543*
HTTPSインスペクションの開始 ... *544*
HTTPSインスペクションポリシー ... *545*
HTTPSインスペクションポリシーの設定 ... *547*
HTTPSインスペクションポリシーの実施 ... *549*
インバウンドCA証明書の操作 ... *549*
インバウンドHTTPSインスペクションのサーバ証明書の割り当て ... *549*
セキュリティゲートウェイでのHTTPSインスペクションの設定 ... *550*
HTTPSインスペクションのデプロイメント図 ... *553*
アウトバウンド CA 証明書の操作 ... *554*
送信CA証明書の作成 ... *554*
アウトバウンドCA証明書のインポート ... *555*
生成されたCA証明書のエクスポートと配置 ... *557*
グループポリシーを使用した証明書の展開 ... *558*
Security Management Serverから別のSecurity Management Serverへの証明書のエクスポート ... *559*
アウトバウンド HTTPS 検査における信頼できる CA との連携 ... *560*
HTTPSインスペクションのグローバル設定 ... *562*
Fail Mode ... *562*
Categorization Mode ... *562*
Server Validations ... *563*
証明書ブロック ... *564*
許可リストをバイパス ... *565*
セッションログ ... *565*

その他 566
中間CA 566
負荷状態のバイパスをログ記録 566
HTTPSインスペクション統計ビュー 567
設定 567
HTTPSインスペクション統計の表示 567
サイト分類のためのSNIサポート 569
非標準ポートでのHTTPSインスペクション 569
TLS v1.3トラフィックのインスペクション 570
HTTP/3 プロトコルのインスペクション (RFC 9114) 570
ルールベースでのHTTPS/3の使用 570
HTTP/3インスペクションのモニタリング 571
制限事項 576
TLS接続のブロック 576
事前準備 576
手順 577
スマートフォンとタブレット向けクライアント証明書 585
クライアント証明書の管理 585
クライアント証明書の作成 586
証明書の取り消し 587
証明書配布用のテンプレートの作成 587
テンプレートの複製 589
クライアント証明書に対する権限の付与 589
環境設定と管理設定 590
データベースの改訂 590
環境のIPアドレスバージョンの設定 593
ウィンドウのデフォルト復元 594
ログインウィンドウの設定 595
ユーザセンターとの同期 596
インスペクションの設定 597

インスペクションの設定 597
SmartTasks 600
使用可能なトリガ 600
利用可能なアクション 602
SmartTaskプロパティの設定 603
SmartTaskの詳細プロパティ 603
Webリクエストの送信 603
スクリプトの実行 603
メール送信 603
IoTデバイス向けネットワークセキュリティ 608
はじめに 608
事前準備 610
ネットワークの概要 610
ネットワーク図 611
IoTサードパーティディスカバリーサービスの設定 611
ポリシーへのIoTアセットの追加 612
IoTログのInfinity 613
ハイアベイラビリティ(HA)管理 615
ハイアベイラビリティ(HA)管理の概要 615
ハイアベイラビリティ環境 616
SmartConsoleでのセカンダリSecurity Management Serverの設定 617
アクティブサーバとスタンバイサーバの同期 619
ハイアベイラビリティのモニタ 619
同期ステータスとアクションのモニタリング 619
サーバをアクティブまたはスタンバイに変更する 621
コリジョンモードでの作業 621
アクティブとスタンバイの切り替え 621
ハイベイラビリティのトラブルシューティング 622
通信していません 622
Collision or HA Conflict(衝突またはHAコンフリクト) 622

Sync Error(同期エラー) 622
Unlocking the Administrator(管理者のロック解除) 622
Endpoint Securityのある環境 623
ハイアベイラビリティのディザスターリカバリ 624
コンプライアンス 626
コンプライアンスビュー 626
コンプライアンススコアリングシステム 627
セキュリティベストプラクティスコンプライアンスビュー 628
ユーザ定義のベストプラクティスの作成 629
ベストプラクティステストの有効化と無効化 632
ゲートウェイビュー 634
ブレードビュー 635
アクションアイテムとメッセージビュー 636
規制コンプライアンスビュー 638
レポートの作成 640
ICA管理ツール 641
メニュー 641
ICA管理ツールへの接続 641
ICA管理ツールポータル 644
ユーザ証明書の管理 645
ユーザ証明書のキーサイズの変更 645
複数の同時操作の実行 646
権限が制限されたICA管理者 647
証明書による運用 648
SIC証明書の管理 648
セキュリティゲートウェイVPN証明書の管理 648
SmartConsoleでのユーザ証明書の管理 648
証明書の初期化に関するユーザへの通知 648
ICA証明書ファイルの取得 648
証明書の検索 648

基本検索パラメータ 649
詳細検索の属性 649
検索結果 650
証明書の詳細の表示と保存 650
証明書の削除と失効、およびEメールによる通知 650
CAへの証明書要求の送信 651
複数の証明書の同時初期化 652
CRL 654
CRLの管理 654
CRLの操作 654
CAプロシージャ 655
CAクリーンアップ 655
CAの設定 655
CAデータタイプと属性 655
証明書の有効期限とステータス 660
Gaia API プロキシ 661
SmartConsoleの新機能のテスト 667
コマンドラインリファレンス 668
CLIコマンドの構文凡例 669
contract_util 671
contract_util check 673
contract_util cpmacro 674
contract_util download 675
contract_util mgmt 677
contract_util print 678
contract_util summary 679
contract_util update 680
contract_util verify 681
cp_conf 682
cp_conf admin 684

cp_conf auto ... 687
cp_conf ca ... 688
cp_conf client ... 690
cp_conf finger ... 694
cp_conf lic ... 695
cp_log_export ... 697
cpca_client ... 713
cpca_client create_cert ... 715
cpca_client double_sign ... 717
cpca_client get_crldp ... 719
cpca_client get_pubkey ... 720
cpca_client init_certs ... 721
cpca_client lscert ... 722
cpca_client revoke_cert ... 725
cpca_client revoke_non_exist_cert ... 728
cpca_client search ... 729
cpca_client set_ca_services ... 732
cpca_client set_cert_validity ... 734
cpca_client set_mgmt_tool ... 735
cpca_client set_sign_hash ... 740
cpca_create ... 742
cpconfig ... 743
cpinfo ... 746
Cplic ... 747
cplic check ... 750
cplic contract ... 752
cplic db_add ... 754
cplic db_print ... 756
cplic db_rm ... 758
cplic del ... 759

cplic del <object name> ... 760
cplic get ... 761
cplic print ... 763
cplic put ... 765
cplic put <object name> ... 768
cplic upgrade ... 771
cppkg ... 773
cppkg add ... 775
ppkg delete ... 777
cppkg get ... 779
cppkg getroot ... 780
cppkg print ... 781
cppkg setroot ... 782
cpprod_util ... 783
cprid ... 787
cprinstall ... 788
cprinstall boot ... 791
cprinstall cprestart ... 792
cprinstall cpstart ... 793
cprinstall cpstop ... 794
cprinstall delete ... 795
cprinstall get ... 796
cprinstall install ... 797
cprinstall revert ... 800
cprinstall show ... 801
cprinstall snapshot ... 802
cprinstall transfer ... 803
cprinstall uninstall ... 804
cprinstall verify ... 806
cpstart ... 808

cpstat ... 809
cpstop ... 816
cpview ... 817
CPViewの概要 ... 817
CPViewユーザインタフェース ... 817
CPViewの使用 ... 818
cpwd_admin ... 819
cpwd_admin config ... 822
cpwd_admin del ... 825
cpwd_admin detach ... 826
cpwd_admin exist ... 827
cpwd_admin flist ... 828
cpwd_admin getpid ... 830
cpwd_admin kill ... 831
cpwd_admin list ... 832
cpwd_admin monitor_list ... 835
cpwd_admin start ... 836
cpwd_admin start_monitor ... 838
cpwd_admin stop ... 839
cpwd_admin stop_monitor ... 841
dbedit ... 842
fw ... 856
fw fetchlogs ... 858
fw hastat ... 861
fw kill ... 862
fw log ... 863
fw logswitch ... 873
fw lslogs ... 877
fw mergefiles ... 880
fw repairlog ... 883

fw sam ... 885
fw sam_policy ... 894
fw sam_policy add ... 897
fw sam_policy batch ... 911
fw sam_policy del ... 913
fw sam_policy get ... 916
fwm ... 922
fwm dbload ... 925
fwm exportcert ... 926
fwm fetchfile ... 927
fwm fingerprint ... 928
fwm getpcap ... 930
fwm ikecrypt ... 932
fwm load ... 933
fwm logexport ... 934
fwm mds ... 939
fwm printcert ... 941
fwm sic_reset ... 947
fwm snmp_trap ... 948
fwm unload ... 951
fwm ver ... 955
fwm verify ... 956
inet_alert ... 957
ldapcmd ... 961
ldapcompare ... 963
ldapmemberconvert ... 967
ldapmodify ... 973
ldapsearch ... 975
mgmt_cli ... 978
migrate ... 979

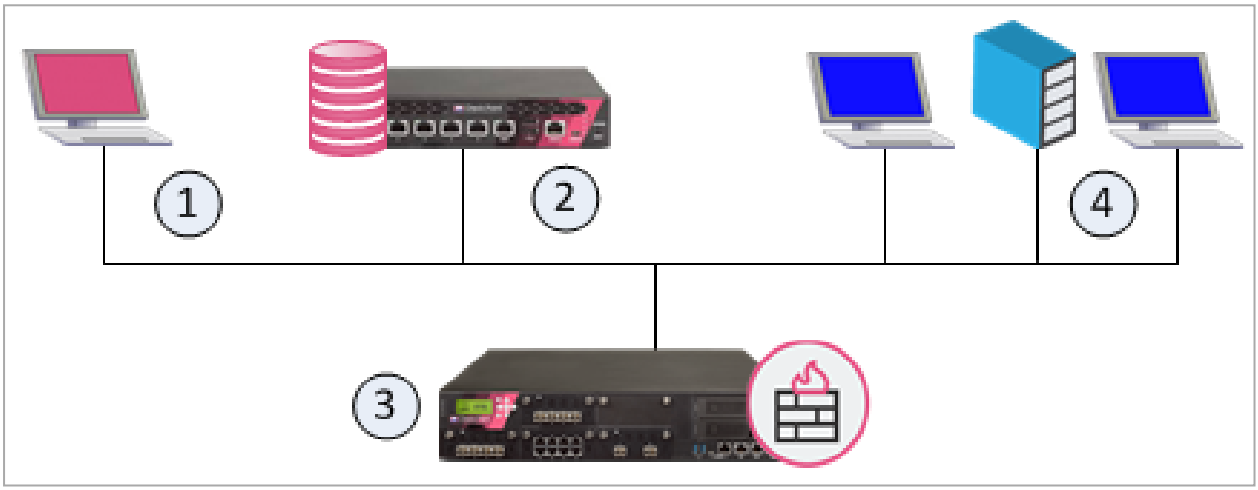
migrate_server ... 983
queryDB_util ... 989
rs_db_tool ... 990
sam_alert ... 992
stattest ... 996
threshold_config ... 999
用語集 ... 1005

Quantum Security Managementについて

Check Pointは、絶えず増大する組織ネットワークのニーズや課題に答えるための、効果的なセキュリティ管理ソリューションを提供しています。この管理ガイドでは、Security Management Serverの基本的な導入に焦点を当てます。

複数のサイトを持つ組織へのデプロイメントに興味がある場合は、以下を参照してください。*R82 Multi-Domain Security Management Administration Guide*。

Check Pointのセキュリティアーキテクチャの基本コンポーネントは、次のとおりです。



項目	説明
1	SmartConsole - Security Management Serverへの接続と管理を行うためのCheck PointのGUI(グラフィカルユーザインタフェース) 。
2	Security Management Server - 定義されたセキュリティポリシーでセキュリティゲートウェイを管理し、ネットワーク上のセキュリティイベントを監視します。
3	セキュリティゲートウェイ - ネットワークトポロジの境界に配置され、セキュリティポリシーの実施により環境を保護します。
4	保護すべき運用環境。

セキュリティ管理設定のワークフロー

1. SmartConsoleでSecurity Management Serverにアクセスします。

   参照: *SmartConsoleでSecurity Management Serverに接続する (33ページ)*。

2. Security Management Serverとセキュリティゲートウェイを環境設定します。

参照: *Security Management Serverとセキュリティゲートウェイの設定 (54ページ)*。

3. 環境の管理者を定義します。

   参照: *管理者アカウントの管理 (74ページ)*。

4. 環境の管理者に権限を割り当てます。

   参照: *管理者への権限プロファイルの割り当て (116ページ)*

5. セキュリティ環境が保護するユーザとユーザグループを定義します。

   参照: *ユーザアカウントの管理 (136ページ)*。

6. 環境内の物理および仮想ネットワークコンポーネントを設定します。

   参照: *オブジェクトの管理 (279ページ)*

7. 組織のリソースの保護を管理するアクセスルールを設定します。

   参照: *アクセスコントロールポリシーの作成 (326ページ)*。

8. セキュリティポリシーをインストールします。

   参照: *アクセスコントロールポリシーのインストール (395ページ)*。

   参照: *脅威対策ポリシーのインストール (514ページ)*。

SmartConsoleパッケージ

SmartConsole は、Check Point Management Serverに接続して、Check Point 環境で必要なオブジェクトやポリシーを設定するために使用するメインの GUI クライアントです。

Check Pointは、これらの SmartConsole パッケージを提供しています:

SmartConsole パッケージ	入手先	説明
デスクトップ SmartConsole	sk181127。	Windows OSベースのコンピュータにインストールする、スタンドアロンのSmartConsoleアプリケーションです。 更新可能なSmartConsoleについては、sk171315 を参照してください。

Web SmartConsole	このパッケージは Management Serverに組み込まれています。
	Management Serverがインターネットに接続されている場合、このパッケージは自動更新可能です。
	sk170314から最新のオフラインパッケージを入手します。
		Web SmartConsoleは、WebブラウザでSmartConsoleのGUI機能を提供します。
		ベストプラクティス- Google Chrome Webブラウザを使用してWeb SmartConsoleに接続することをお勧めします。
		Web SmartConsoleに接続します:
		1. Webブラウザで、次に接続します。
		`https://<IP Address of the Management Server>/smartconsole`
		例:
		`https://192.168.3.57/smartconsole`
		2. 管理サーバの管理者の認証情報でログインします。

ポータブル SmartConsole	sk116158。	ポータブルSmartConsoleは、SmartConsoleのインストーラを使用せずに導入できるSmartConsoleクライアントのバージョンです。 このパッケージは、すべてのコンテンツを配置されるディレクトリにカプセル化し、ポータブルデバイスで持ち運べるようにします。 このバージョンのもう1つの利点は、同じコンピュータ上で同じリリースのSmartConsoleを並べて使用できることです。

SmartConsoleでSecurity Management Serverに接続する

SmartConsoleでSecurity Management Server/ドメイン管理サーバにログインするには、Security Management Server/ドメイン管理サーバに管理者アカウントを設定する必要があります。

Security Management Server/マルチドメインSecurity Management Serverのインストール時に、初期設定ウィザードで管理者を1人作成します。その後、SmartConsoleに管理者アカウントを追加作成できます。

SmartConsoleでSecurity Management Server/ドメイン管理サーバにログインするには

1. SmartConsoleアプリケーションを起動します。

   参照: *SmartConsoleパッケージ (32ページ)*。

2. 管理者認証情報を入力します。

   ユーザ名、*証明書ファイル*、*CAPI証明書*などです。

   - *ユーザ名でのログイン:*

     Usernameと**Password**を入力します。

   - *証明書ファイルによるログイン*

     a. ドロップダウンリストから、**Certificate File**を選択します。

     b. ファイルを参照します。

        これは、管理者オブジェクトで作成した証明書ファイルです。

        参照: *管理者アカウントの管理 (74ページ)*。

     c. 証明書ファイルのパスワードを入力します。

   - *CAPIリポジトリの証明書でログイン:*

     前提条件 - SmartConsoleの管理者オブジェクトで証明書ファイルを作成し、保存して、SmartConsoleクライアントコンピュータのWindows証明書ストアにインポートすることが重要です。参照: *管理者アカウントの管理 (74ページ)*。

     a. ドロップダウンリストから、**CAPI Certificate**を選択します。

     b. ドロップダウンリストから、管理者を選択します。

- *Identity Providerでログイン:*

  ドロップダウンリストから「Identity Provider」を選択します。

  注 - 認証情報を入力する必要はありません。接続しているサードパーティのIDプロバイダでは、すでに認識、認証されています。IDプロバイダの設定方法については、以下を参照。*SAML認証ログインによる管理者アカウントの作成 (101ページ)*。

3. Security Management Server/Domain Management Serverの名前またはIPアドレスを入力します。
4. 読み取り専用モードで接続するには、**Read Only**チェックボックスを選択します。
5. **Login**をクリックします。

   SmartConsoleは、Security Management Server/Domain Management Serverを認証します。初回接続時は、SmartConsoleにフィンガープリントが表示されます。
6. フィンガープリントを確認します。

フィンガープリントとSecurity Management Server/Domain Management ServerのIPアドレスは、Windowsのユーザ設定に保存されます。

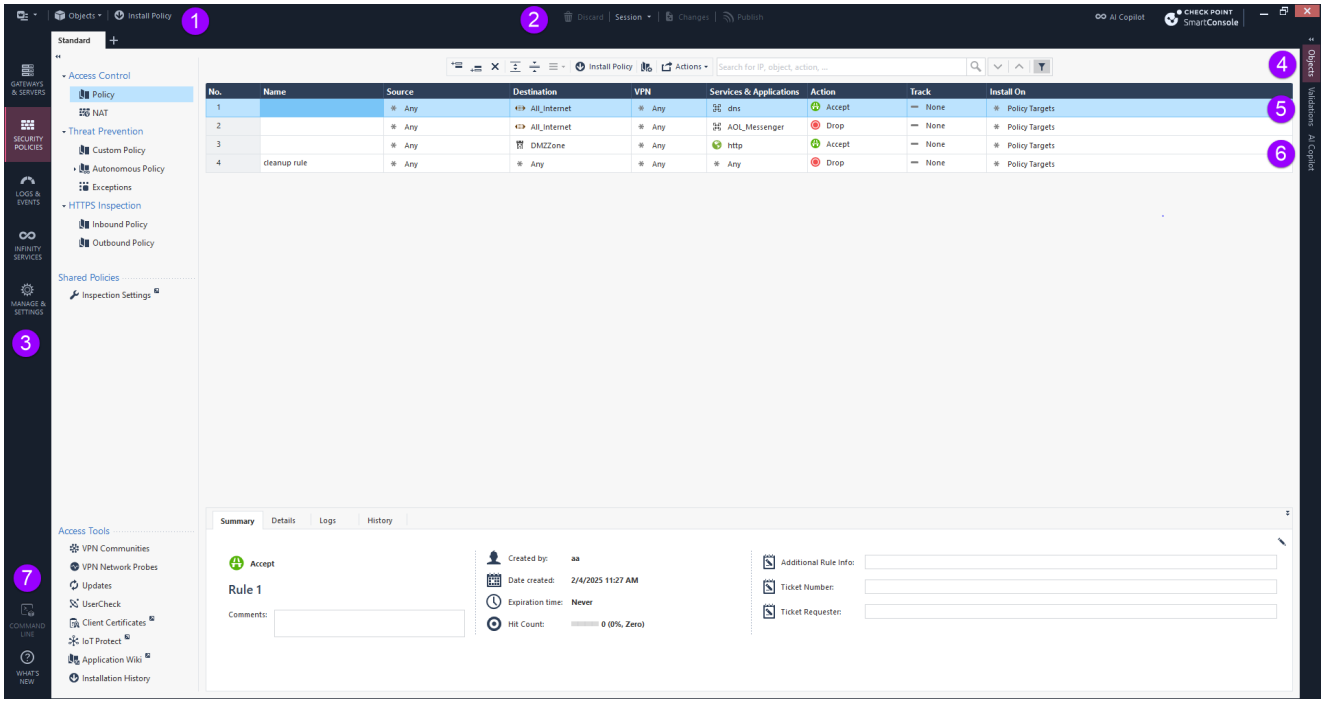
SmartConsoleを理解する

Check Point SmartConsoleは、複雑なネットワークのセキュリティを簡単に管理するためのツールです。サイバーセキュリティ環境とポリシーを設定する前に、Check PointのSmartConsoleについてよく理解しておいてください。

SmartConsoleパッケージは、ホームページSKの記事で入手できます。sk181127.

SmartConsoleのパッケージは、英字のみを含むフルパスのフォルダにインストールする必要があります。

SmartConsoleウィンドウ

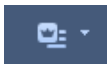


項目	説明	項目	説明
1	グローバルツールバー	5	検証ペイン
2	セッション管理ツールバー	6	AI Copilot。詳しい説明と最低要件については、sk182844を参照。
3	ナビゲーションツールバー	7	コマンドライン・インタフェース・ボタン
4	オブジェクトバー (F11)		

注 - SmartConsole > **Gateways & Servers**ビューで、上部ツールバーの**Filter** (漏斗)ボタンをクリックした後、各カテゴリ(バージョン、ハードウェアなど) で1つのファセットのみを選択できます。

SmartConsoleのツールバー

グローバルツールバー(SmartConsoleの上部)

アイコン	説明
	SmartConsoleのメインメニューです。SmartConsoleがSecurity Management Serverに接続されている場合、以下があります。 ■ ポリシーとレイヤーの管理 ■ オブジェクトエクスプローラを開く ■ 新しいオブジェクト(新しいオブジェクトを作成するメニューを開く) ■ セッションの公開 ■ セッションを破棄 ■ セッションの詳細 ■ ポリシーインストール ■ アクセスコントロールポリシーの検証 ■ データベースのインストール ■ Threat Preventionポリシーのアンインストール ■ ハイアベイラビリティ(HA) 管理 ■ ライセンスとパッケージの管理 ■ エンドポイント (SmartEndpointとHarmony Endpoint Web UIへのメニューを開く) ■ グローバルプロパティ ■ ビュー(開くビューを選択するメニューを開く)
	新規オブジェクトの作成、またはオブジェクトエクスプローラを開く
	マネージドセキュリティゲートウェイにポリシーをインストールする

セッション管理ツールバー(SmartConsoleの上部)

アイコン	説明
	セッション中に行われた変更を破棄する
	セッションの詳細を入力すると、そのセッションで行われた変更回数が表示されます。
	SmartConsoleセッションを公開し、他の管理者が変更内容を確認できるようにし、セキュリティゲートウェイにインストールできるようにします。 **注** - ポリシーがインストールされると、公開された変更がSecurity Gatewayにインストールされ、強制的に実行されます。

ナビゲーションツールバー(SmartConsoleの左側)

アイコン	キーボードショートカット	説明
	Ctrl+1	**Gateways & Servers**設定ビュー: ■ セキュリティゲートウェイの管理 ■ Software Bladesのアクティベーション ■ セキュリティゲートウェイおよびクラスタ(仮想クラスタを含む) の追加、編集、および削除 ■ スクリプトの実行 ■ セキュリティゲートウェイのバックアップと復元 ■ セキュリティゲートウェイでコマンドラインインタフェースを開く ■ セキュリティゲートウェイのステータスを表示
	Ctrl+2	セキュリティポリシー アクセスコントロールビュー: ■ アクセスコントロールの管理コンテンツアウェアネス、VPN、アプリケーション& URLフィルタリング、モバイルアクセス ■ 複数のポリシーの同時編集 ■ NATルールの追加、編集、削除 ■ アクセスツールを使う セキュリティポリシーThreat Preventionビュー: ■ 脅威対策の管理:IPS、アンチボット、アンチウイルス、Threat Emulation ■ 統合脅威ルールベースの編集 ■ 脅威プロファイルの設定 ■ 例外および例外グループの追加、編集、削除 ■ カスタムポリシーツールを使用する 共有ポリシービュー: ■ モバイルアクセス、DLP、インスペクション設定の管理
	Ctrl+3	ログ&イベントビュー: ■ ハイレベルなグラフやプロットの表示 ■ ログの検索 ■ カスタマイズされたレポートのスケジュール ■ セキュリティゲートウェイの監視 ■ コンプライアンス情報の表示

アイコン	キーボードショートカット	説明
	Ctrl+4	Infinity Servicesビュー: ■ オンプレミスの管理サーバからInfinity Portalへの接続 ■ Infinity Portalで管理されているサービスを、管理サーバオブジェクト上で実行します。 ■ クラウドとオンプレミスの両方で、すべてのCheck Point製品の統合ログビューを確認できます。 ■ オンプレミスの管理サーバで新しい管理者機能を使う
	Ctrl+5	Manage & Settingsビュー - Security Management Serverの設定の確認と設定: ■ 管理者 ■ 権限プロファイル ■ 信頼できるクライアント ■ 管理者セッション、およびセッションの設定 ■ ブレード ■ 改訂 ■ プリファレンス ■ ユーザセンターとの同期

コマンドラインインタフェースボタン(SmartConsoleの左下隅)

アイコン	キーボードショートカット	説明
	F9	管理用スクリプトやAPIのコマンドラインインタフェースを開く

その他のSmartConsoleショートカットについては、以下を参照してください。*SmartConsoleのキーボードショートカット (48ページ)*。

オブジェクトバー(SmartConsoleの右側)

項目	キーボードショートカット	説明
オブジェクト	F11	セキュリティとネットワークオブジェクトの管理

AI Copilot ペイン(SmartConsoleの右 側

項 目	説 明
AI Copilot	Infinity AI CopilotはSmartConsoleに統 合 されたインテリジェントなアシスタントで、タスクを効 率 化し、実 用 的なインサイトを提 供して効 率 的なセキュリティ管 理を実 現 するように設 計 されています。詳しい説 明と最 低 要 件については、sk182844を参 照 。

検 証 ペイン(SmartConsoleの右 側)

項 目	説 明
検 証	検 証 エラーの表 示

システム情 報 エリア(SmartConsoleの下 部)

項 目	説 明
タスクリスト	進 行 中 の管 理 タスク。最 近 のタスクを表 示 するために拡 大 する
サーバの詳 細	SmartConsoleが接 続 されているサーバのIPアドレス。Management High Availabilityが設 定 されている場 合 、クリックして詳 細 を表 示 します。
セッションステータス	セッションで行 われた変 更 回 数 とセッションの状 態 。
接 続 管 理 者	接 続 管 理 者 : 自 分 と他 の管 理 者

検索エンジン

各ビューでは、Security Management Serverのデータベースを検索して、そのビューに関連する情報を得ることができます。例：

- 名前またはIPアドレスによるゲートウェイ
- アクセスコントロールルール
- NAT ルール
- 脅威対策プロファイル
- 特定の脅威または脅威のカテゴリ
- オブジェクトタグ

Security Management Serverデータベース内のオブジェクトを検索するには、次の2つの方法があります。

- オブジェクト名のプレフィックスを入力します。例えば、*USGlobalHost*を見つけるには、検索ボックスに*USG*と入力します。
- オブジェクト名に任意の文字列を入力し、その前にアスタリスク(*) を付けます。

  たとえば、*USGlobalHost*を見つけるには、検索ボックスに**oba*、**host*、**SG*などを入力します。

IP検索

IPアドレス、ネットワーク、ポートの詳細検索が可能です。検索条件に直接一致するものと間接的に一致するものを返します。

- IPアドレス: xxx.xxx.xxx.xxx
- ネットワーク: xxx.xxx.0.0/16 または xxx.xxx
- ポート：svc:<xxx>

IP検索モードの違い:

- **一般** - (デフォルト)。IP範囲、ネットワーク、グループ、除外を含むグループ、およびこれらのオブジェクトを含むルールで直接マッチした結果と間接的な結果を返します。
- **パケット** - 使用するIPアドレスのパケットがセキュリティゲートウェイに到着したかのようにルールにマッチします。

一般的なIP検索

これはデフォルトの検索モードです。ルールベース内やオブジェクト内の検索に使用します。有効なIPやネットワークでない文字列を入力した場合、検索エンジンではテキストとして扱われます。

有効なIPアドレスまたはネットワークを入力すると、次のオブジェクトとルールについて、高度な検索が行われます。

- IPアドレスをコメントなどのテキスト値として持っているオブジェクト
- IPアドレスプロパティを持つオブジェクト(直接の結果)
- テキスト値またはアドレス値を持つオブジェクトを含むグループ、ネットワーク、およびアドレス範囲
- それらのオブジェクトを含むルール

パケットサーチ

パケットサーチは、使用するIPアドレスのパケットがセキュリティゲートウェイに到着したかのようにルールにマッチします。

次を持っているルールにマッチします。

- ルールのカラムに含まれるIPアドレス
- "Any"
- IPアドレスを宣言に含むGroup-with-exclusionまたはnegatedフィールド

パケットサーチを実行するには

1. 検索ボックスをクリックします。

   検索ウィンドウが開きます。

2. **Packet**をクリックするか、"mode:Packet"と入力します。
3. 特定のルールカラムを検索するには、次のように入力します: *ColumnName:Criteria*

ルールベース結果

検索条件を入力し、マッチした結果を表示すると、ルール内の条件にマッチした値がハイライト表示されます。

次がある場合...	強調表示されるもの
オブジェクト名またはテキストカラムの直接一致	マッチした特定の文字のみ
オブジェクトのプロパティに直接一致	オブジェクト名全体
ネゲート カラム	ネゲート ラベル
"Any "でのマッチング	"Any"

既知の制限:

- パケットの検索はIPv6をサポートしていません。

アクセス、カスタム、HTTPSインスペクションツール

Security Policies Access ControlビューのAccess ToolsセクションとSecurity Policies Threat PreventionビューのCustom Policy Toolsセクションには、さらに多くの管理ツールやデータ収集ツールがあります。

セキュリティポリシー"アクセスコントロール"ビューの"アクセスツール"

ツール	説明
VPN Communities	VPNコミュニティの作成、編集、削除。
VPN Network Probes	サイト間VPNトンネルのステータスと可用性をモニタします。
Updates	アプリケーション＆ URLフィルタリングデータベースのアップデート、アップデートのスケジュール、アップデートの設定。
UserCheck	アクセスコントロール ポリシーアクション用にUserCheck Interactionオブジェクトを設定。
Client Certificates	ユーザがハンドヘルドデバイスからセキュリティゲートウェイに認証するためのクライアント証明書の作成、配布。
IoT Protect	IoTデバイスのネットワークIoTセキュリティを設定。
Application Wiki	Check Point AppWikiを参照。Web 2.0 Applications Databaseの検索とフィルタリングにより、アプリケーション、アプリ、ウィジェットに対するアクションのポリシールールにCheck Pointのセキュリティリサーチ結果を利用可能。
Installation History	各セキュリティゲートウェイのポリシーのインストール履歴と、誰が変更したかを確認可能。各インストール時に行われたリビジョンと、そのリビジョンを行った人を確認可能。特定のバージョンのポリシー インストール。

セキュリティポリシー「脅威対策」ビューの「カスタムポリシーツール」

ツール	説明
Profiles	プロファイルの作成、編集、削除。
IPS Protections	各プロファイルごとのIPS保護の編集。
Protections	各種プロテクションの統計を確認。

ツール	説明
Allow List Files	ホワイトリストのファイルリストの設定。
Indicators	悪意のある活動の指標とその対処方法の設定。
Updates	マルウェアデータベース、Threat Emulationエンジンおよびイメージ、IPSデータベースの更新の設定。
UserCheck	脅威対策ポリシーアクションのUserCheck Interactionオブジェクトを設定。
Threat Wiki	Check Point ThreatWikiの参照。Check Pointのマルウェアデータベースの検索とフィルタリングで、マルウェアが環境に侵入する前にブロックし、侵入された場合は最適な対処を行うことが可能。
Installation History	各セキュリティゲートウェイのポリシーのインストール履歴と、誰が変更したかを確認可能。各インストール時に行われたリビジョンと、そのリビジョンを行った人を確認可能。特定のバージョンのポリシーインストール。

セキュリティポリシー HTTPSインスペクションビューの HTTPSインスペクションツール

ツール	説明
デプロイメント	学習モードで HTTPSインスペクションが有効になっているセキュリティゲートウェイのステータスと推奨事項を参照。各セキュリティゲートウェイのインスペクションステータスを確認。セキュリティゲートウェイのインバウンドおよびアウトバウンド証明書を管理。
Advanced Settings	すべてのセキュリティゲートウェイに対してHTTPSインスペクションのグローバル設定を行う。
Trusted Certificates	信頼されたCAおよびカスタム信頼された証明書を管理する。

共有ポリシー

Security Policiesの**Shared Policies**セクションには、ポリシーパッケージに含まれないポリシーが表示されます。これらは、すべてのポリシーパッケージで共有されます。

共有ポリシーは、アクセスコントロールポリシーと一緒にインストールされます。

Software Blade	説明
Mobile Access	SmartConsoleでモバイルアクセスポリシーを起動します。リモートユーザがモバイルでメールアカウントなどの社内リソースにアクセスする方法を設定します。
DLP	SmartConsoleでData Loss Preventionポリシーを起動します。ネットワーク外に漏れてはならないデータを自動的に特定し、漏えいをブロックし、ユーザを教育するための高度なツールを設定します。
Inspection Settings	セキュリティゲートウェイのインスペクションの設定ができます(*環境設定と管理設定 (590ページ)*): ■ ディープパケットインスペクションの設定 ■ プロトコル解析のインスペクション設定 ■ VoIPパケットインスペクションの設定

APIコマンドラインインタフェース

SmartConsoleからアクセスできるAPIコマンドラインインタフェースからでも、オブジェクトやルールを設定することができます。

	クリックすると、コマンドラインインタフェースが開きます。
	コマンドラインインタフェースでは、このボタンをクリックするとCheck Point Management API Referenceが開きます。 Check Point Management API Referenceは、Check Point Management APIの使用方法に関する詳細な情報を提供する包括的なガイドです。

コマンドラインインタフェースに加えて、APIスクリプトを作成して実行することで、Security Management Server上の設定や操作を管理することができます(以下のセクションを参照)。*APIによるセキュリティ管理 (56ページ)*)。

SmartConsoleのキーボードショートカット

これらは、SmartConsoleの各フィールド間を移動するために使用できる追加のキーボードショートカットです:

キーボードショートカット	説明
Ctrl+S	SmartConsoleセッションを公開する。
Ctrl+Alt+S	SmartConsoleセッションを破棄
Shift+Alt+Enter	ポリシーのインストール
F10	タスクの詳細の表示/非表示。
F11	オブジェクトエクスプローラの表示/非表示。
Ctrl+O	ポリシーとレイヤーの管理
Ctrl+E	オブジェクトエクスプローラを開く
Ctrl+F3	ハイコントラストのテーマに切り替え
Alt+Space	システムメニュー
F1	該当するオンラインヘルプを開く
Alt+F4	SmartConsoleを閉じる

サポートする特定のビューのショートカット

キーボードショートカット	説明
Ctrl+T	新しいタブを開く
Ctrl+WまたはCtrl+F4	現在のタブを閉じる
Ctrl+Tab	次のタブに移動
Ctrl+Shift+Tab	前のタブに移動
削除	現在選択されているアイテムを削除する
Ctrl+A	すべてのエレメントを選択する
Esc	操作をキャンセルしてウィンドウを閉じる
Enterキーまたはマウスをダブルクリック	アイテムの編集

セキュリティポリシービューで、ポリシーが含まれるページのショートカット：

キーボードショートカット	説明
Ctrl+G	ルールへ移動(アクセスコントロールルールベース内)
Ctrl+X	ルールの切り取り
Ctrl+C	ルールのコピー
Ctrl+V	選択したルールの下にルールを貼り付け
削除	ルールセルから使用済みのアイテムを削除する
Ctrl+F	ルールベース検索を開く
F3	次のルールベース検索結果へ移動する
Ctrl+上矢印キー	ルールベースの最初のルールに移動する
Ctrl+下矢印キー	ルールベースの最後のルールに移動する
スペースまたは+	ルールベースの現在のセルのドロップダウンメニューを開く
Shift+上/下矢印	ルールベース内のオブジェクト間の移動

ログ＆イベントビューのショートカット：

キーボードショートカット	説明
Ctrl+G	グリッドビューに切り替える(ログビュー、監査ログビュー)
Ctrl+L	テーブルビューに切り替える(ログビュー、監査ログビュー)
Ctrl+R	オブジェクトの解決
F5	クエリの更新
F6	自動リフレッシュを有効にする
Ctrl+D	お気に入りに追加
Ctrl+S	お気に入りの整理

SmartConsoleでのInfinity AI Copilotの使用

Infinity AI CopilotはSmartConsoleに統合されたインテリジェントなアシスタントで、タスクを効率化し、実用的な洞察を提供して効率的なセキュリティ管理を実現するように設計されています。

Infinity AI Copilotは、Check Pointのセキュリティポリシー、順序付けられたレイヤーとインラインレイヤーの仕組み、セキュリティゲートウェイがトラフィックをルールに適合させる仕組み、ログの照会方法などを理解し、読み取るように訓練されています。また、管理ガイドやナレッジベースSKの内容に基づいてInfinity AI Copilotは学習しています。そのため、Infinity AI Copilot はCheck Pointの環境について的確な回答ができます。

Security Management ServerをInfinity Portalに接続すると、Infinity AI Copilotは、Security Management Server上の設定済みオブジェクト、セキュリティポリシー、ログ(ログ共有を有効にした場合)を読み取り、環境に関する質問に答えることが可能です。

事前準備

Desktop SmartConsoleの要件	Web SmartConsoleの要件
Desktop SmartConsoleでInfinity AI Copilotを使用するには、以下の2つのパッケージをインストールする必要があります: 1. Desktop SmartConsole Build 1027以降。 2. Web SmartConsole Take 125 or higher。	Web SmartConsoleでInfinity AI Copilotを使用するには、このパッケージをインストールする必要があります: Web SmartConsole Take 125 or higher

注 - Web SmartConsoleは常に最新のものをインストールすることをお勧めします。

Infinity AI Copilotを有効にするには

1. Security Management ServerをInfinity Portalに接続します。

   参照: *SmartConsole から Infinity Portalに Security Management Server および セキュリティゲートウェイ オブジェクトを接続するには、次の手順に従います。(538ページ)*。

2. Infinity AI Copilotを有効にする:

a. Infinity ServicesページのInfinity AI Copilotウィジェットで、トグルを**ON**に変更します。

b. 画面の指示に従います。

Infinity AI CopilotタブがSmartConsoleの右パネル(および右上) に表示されます。

3. オプション: ログについて質問するには、ログを共有する必要があります。

参照: *オンプレミスの管理サーバのログ情報をInfinity Portalで共有するには (539ページ)*。

Security Managementの計画

Security Management Serverのサイズ

このセクションでは、Security Management Serverのサイジングや既存環境のサイジングの検証に役立つ情報を提供します。

Security Management Serverの正確なサイジングに必要なデータ:

- Security Management Serverが管理するセキュリティゲートウェイの数。
- 1秒あたりの持続ログ。
- 大規模なデプロイメント:
  - ドメイン数
  - ルールベースのサイズ
  - 同時管理者数
  - セキュリティ管理の制限

データを収集し、管理サーバの適切なサイズを特定する方法については、sk181782にガイドラインがあります。

マルチドメイン/大規模デプロイメントについては、sk178325を参照してください。

推奨:

- 専用の管理サーバを使用する。
- 専用のログサーバを使用する。
- Management High Availabilityを構成する。スタンバイ管理サーバをゲートウェイのログサーバとして使用できます。
- 専用のSmartEvent Serverを使用します。
- ゲートウェイのプライマリログサーバとしてSmartEvent Serverを定義できます(マルチドメインセキュリティ管理構成には適用されません) 。

Security Management Serverとセキュリティゲートウェイのインストールが完了したら、引き続き運用環境に合わせたサイバーセキュリティの設定を行うことができます。

組織のトポロジの定義

ネットワークトポロジは、物理的および論理的なネットワークコンポーネント(物理および仮想のセキュリティゲートウェイ、ホスト、ハンドヘルドデバイス、CAサーバ、サードパーティサーバ、サービス、リソース、ネットワーク、アドレスレンジ、グループなど)で構成されています。これらのコンポーネントはそれぞれ、Check Pointのセキュリティ管理構成におけるオブジェクトに対応しています。SmartConsoleでそれらのオブジェクトを設定します。参照: *ネットワークオブジェクトの種類 (284ページ)*。

セキュリティ環境で保護するユーザとユーザグループの定義

データベースへのユーザやグループの追加は、LDAPやUser Directory、またはActive Directoryを使って手動で行うことができます。

ユーザとユーザグループを追加するには*ユーザアカウントの管理 (136ページ)*

LDAPとユーザディレクトリを使用するには、以下を参照してください。*外部LDAPサーバ上のユーザの設定 (218ページ)*。

Active Directoryを使用するには、以下を参照してください。*Microsoft Active Directory (218ページ)*。

組織のリソースを保護するためのアクセスルールの定義

アクセスルールを設定し、セキュリティゲートウェイに適用されるポリシーにグループ化します。トラフィック、アプリケーション、Webサイト、およびデータに基づいてアクセスポリシーを定義できます (*ポリシーの管理 (315ページ)*)。Check Point Anti-VirusおよびAnti-Malwareを使用して、既知の脅威に対する予防措置を設定します。UserCheckを利用して、ユーザが行う操作の妥当性と安全性を教育します。ログ記録とモニタリングを通して、ネットワークトラフィックとイベントを追跡します。

アクセスポリシーの実施

セキュリティゲートウェイを設定します。適切なSoftware Bladesが有効になっていることを確認します。その後、セキュリティゲートウェイにポリシーをインストールします。

Security Management Serverとセキュリティゲートウェイの設定

セキュリティ環境の設定を開始するには、Security Management Serverとセキュリティゲートウェイの設定を行います。セキュリティゲートウェイでは、Security Management Serverで定義したセキュリティポリシーを実施します。

SmartConsoleでSecurity Management Serverを設定するには

1. **Gateways & Servers**ビューで、Security Management Serverオブジェクトを見つけます。

   ビューの上部にある**Search**ボックスでは、オブジェクト名またはオブジェクトのIPアドレスで検索することができます。

   Security Management Serverオブジェクトを選択すると、下部ペインの**Summary**タブに、有効になっているSoftware Bladesが表示されます。

2. オブジェクトをダブルクリックして、プロパティを表示します。

   Managementタブで、必要に応じてSoftware Bladeを有効にします。

   - **Network Policy Management**- すべてのセキュリティ機能に対して統一された、包括的なセキュリティポリシーを管理します。これは自動的に有効になります。
   - **Endpoint Policy Management**- エンドユーザコンピュータおよびハンドヘルドデバイス上のエンドポイントセキュリティクライアントを管理します。

     重要 - このSoftware Bladeを有効にした後に無効にすることはサポートされていません。

   - **Logging & Status**- セキュリティゲートウェイ、VPN、ユーザなどのセキュリティイベントやステータスを、高度なビジュアルとデータ管理機能でモニタします。
   - **Identity Logging**- Active Directoryドメインから、ユーザID、およびユーザのコンピュータやデバイスのデータをログエントリに追加します。
   - **User Directory**- セキュリティスコープに、環境内のLDAPサーバからユーザアカウントを入力します。
   - **Provisioning**- 複数のアプライアンスとオープンサーバのセキュリティゲートウェイの設定とポリシーを1つのSmartConsoleで集中管理。
   - **Compliance**- セキュリティ設定の最適化と規制要件の遵守
   - **SmartEvent Server**- セキュリティイベントをリアルタイムで管理
   - **SmartEvent Correlation Unit**- セキュリティイベントをリアルタイムで関連付け。

SmartConsoleでセキュリティゲートウェイを設定するには

1. ナビゲーションツールバーから、**Gateways & Servers**を選択します。
2. **New**をクリックし、**Gateway**を選択します。
3. 開いた**Check Point Security Gateway Creation**ウィンドウで、設定モードを選択します。
   - **Wizard Mode**- 設定ウィザードを実行します。
   - **Classic Mode**- クラシックモードでセキュリティゲートウェイの設定を行います。*ゲートウェイの管理 (222ページ)*)。

APIによるセキュリティ管 理

ここでは、Management Server上 のAPI Serverと、利 用 可 能なAPIツールについて説 明します。

API

Management Server上 で動 作 するAPI Serverに送 信 するAPI Requestを通じて、Management Serverの設 定 や制 御 を行うことができます。

API Serverは、日 々 の作 業 を自 動 化 するスクリプトを実 行し、Check Pointのソリューションを仮 想 化 サーバ、チケットシステム、変 更 管 理システムなどのサードパーティ製 システムと統 合します。

管 理APIについての詳 細 、コードサンプル、ユーザフォーラムの活 用については、次を参 照ください。

- APIドキュメント :
  - オンライン - *Check Point Management API Reference*
  - ローカル - `https://<Server IP Address>/api_docs`

    デフォルトでは、ローカルAPIドキュメント へのアクセスは無 効になっています。sk174606の指 示に従ってください。

    注 - スタンドアロンサーバ(Security Management Serverとセキュリティゲートウェイの両 方を実 行するサーバ)では、SmartView Webアプリケーション(`https://<Server IP Address>/smartview`)を開くとWeb Portal(`https://<Server IP Address>/api_docs`)が機 能しなくなります。
- **Developers Network**セクション*Check Point CheckMates Community*。

APIツール

これらのツールを使って、Management Server上のAPI Serverを操作することができます。

- Gaiaオペレーティングシステムに備えられたスタンドアロン管理ツール:

  `mgmt_cli`

- SmartConsoleに含まれるスタンドアロン管理ツール:

  `mgmt_cli.exe`

  このツールは、SmartConsoleのインストールフォルダから、Windowsオペレーティングシステムが動作する他のコンピュータにコピーできます。

- クライアントと管理サーバ間で、HTTPプロトコルによる通信とデータ交換を可能にするWebサービスAPI。

  また、これらのAPIを使用して、Check Pointの他のプロセスがHTTPSプロトコルを介してManagement Serverと通信することもできます。

  `https://<IP Address of Management Server>/web_api/<command>`

APIサーバの設定

APIサーバを設定するには

1. SmartConsoleでSecurity Management Serverまたは該当するDomain Management Serverへ接続します。
2. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。
3. 左上のセクションで、**Blades**をクリックします。
4. **Management API**セクションで、**Advanced Settings**をクリックします。

   Management API Settingsウィンドウが開きます。
5. **Startup Settings**と**Access Settings**を設定します。

スタートアップ設定

Automatic startを選択すると、Management Serverを起動または再起動したときにAPI Serverが自動的に起動します。

注:
- 管理サーバに4GB以上のRAMがインストールされている場合、管理サーバのインストール時に**Automatic start**オプションがデフォルトで有効になります。
- 管理サーバのRAMが4GB未満の場合、**Automatic start**オプションは無効になります。

アクセス設定

APIサーバに接続できるクライアントを設定するには、以下のオプションのいずれかを選択します。

- **Management server only**

  APIサーバに接続できるのは、管理サーバだけです。

  このオプションは、管理サーバのコマンドラインで`mgmt_cli`ユーティリティを使用してAPIリクエストを送信することのみを許可します。

  SmartConsoleやWebサービスを使用して、APIリクエストを送信することはできません。

- **All IP addresses that can be used for GUI clients**

  SmartConsole >**Permissions & Administrators** >**Trusted Clients** で定義されているすべてのIPアドレスからAPIリクエストを送信できます。

  これには、SmartConsole、Webサービス、およびManagement Server上の`mgmt_cli`ユーティリティからのリクエストが含まれます。

- **All IP addresses**

  すべてのIPアドレスからAPIリクエストを送信できます。

  これには、SmartConsole、Webサービス、およびManagement Server上の`mgmt_cli`ユーティリティからのリクエストが含まれます。

6. クリック**OK**。
7. 左上のセクションで、**Permissions & Administrators**をクリックします。
8. 該当する各管理者のオブジェクトで、割り当てられた権限プロファイルが管理アプリケーションAPIへのアクセスを許可していることを確認します。

手順

a. 管理者オブジェクトを編集します。

b. 左のパネルで**General**をクリックします。

c. **Permissions**セクションで、選択した権限プロファイルの右側にある目のアイコンをクリックします。

権限プロファイルオブジェクトは読み取り専用ビューで開きます。

d. 左のパネルで**Management**をクリックします。

e. 権限**Management API Login**を選択します。

選択されていない場合は、このウィンドウを閉じて、この権限プロファイルオブジェクトを編集します。

詳細: *管理者への権限プロファイルの割り当て (116ページ)*。

f. クリック**Close**。

9. SmartConsoleセッションを公開する。

10. このコマンドで、Management Server上のAPI Serverを再起動します。

```
api restart
```

注:

- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

- このコマンドの出力:

```
API started successfully
```

11. このコマンドを使用して、管理サーバ上のAPIサーバのステータスを調べます:

```
api status
```

注:

- このコマンドの出力:

```
-------------------------------------------
Overall API Status: Started
-------------------------------------------

API readiness test SUCCESSFUL. The server is up and ready
to receive connections
```

- このコマンド出力には、"API"プロセスの状態が"Stopped"に設定され(APIアクセスが**GUIクライアントに使用できるすべてのIPアドレス**に設定)、200以上のTrusted Clientが設定されている場合があります:

```
Processes:

Name       State     PID       More Information
-----------------------------------------------
API        Stopped   ...
```

セルフマネージドセキュリティゲートウェイ

はじめに

R82は、高度に自動化されたネットワーク(動的環境を持つ顧客を支援するため、アクセスコントロールポリシーに新しいダイナミックレイヤーを導入しました。

このポリシーレイヤーは、Gaia APIコール「`set-dynamic-content`」を使用してセキュリティゲートウェイ上で直接作成されたルールのコンテナとして機能し、JSONファイルの配布を通じてプロビジョニング、コンフィギュレーション、その他のITプロセスが定期的に管理される環境に対応します。

ワークフロー:

1. 管理サーバのアクセスコントロールで、新しいポリシーレイヤーを作成し、ダイナミックレイヤーとして設定します。
2. セキュリティゲートウェイでは、Gaia APIコール「`set-dynamic-content`」(JSON形式)を使って、このダイナミックレイヤーに必要なアクセスコントロールルールを設定します。

ダイナミックレイヤーは、セキュリティゲートウェイで設定したルールのコンテナとしてのみ機能します。セキュリティゲートウェイでGaia APIコマンドを実行すると、SmartConsoleで設定されたダイナミックレイヤーのルールはすべて無視されます。永続的なルールが必要な場合(リモートAPIクライアントからのアクセスを許可する場合など)、ダイナミックレイヤーではなく、管理サーバのメインポリシーで設定する必要があります。

詳細はsk182252を参照。

必要条件

1. 管 理 サーバR82以 降 :
   - Security Management Server
   - Multi-Domain Security Management Server
2. セキュリティゲート ウェイR82以 降 :
   - 単 一 セキュリティゲート ウェイ
   - ElasticXL Cluster
   - ClusterXL
   - Maestroまたはスケーラビリティのあるシャーシのセキュリティグループ
3. セキュリティゲート ウェイでは、Gaia APIを実 行 するユーザがGaia OSでこの設 定 を行 っている必 要 があります :
   a. **ロール**: `adminRole`。
   b. **アクセスメカニズム**: Gaia API。
   c. **シェル**: `/bin/cli.sh or /bin/bash`

   詳 細 は*Gaia Administration Guide*バージョン> **ユーザ管 理** の章 > **ユーザとロール**のセクション。

制限事項

- この機能はJSONフォーマット用に設計されました。

  必要なAPI本体をJSON形式で貼り付けることができる、サードパーティのREST APIクライアントを使用します。

  Check Point CLI API クライアント「`mgmt_cli`」は使用しないでください。

- セキュリティゲートウェイ上の個々の動的ルールを追加後に編集または削除することはサポートされていません。

  - 個々の動的ルールを変更するには、アクセスコントロールルール全体と、その個々のルールの更新されたパラメータと値を含む更新されたAPIボディで、Gaia APIコール "`set-dynamic-content`" を実行する必要があります。
  - 個々の動的ルールを削除するには、その個々のルールを含まない完全なアクセスコントロールルールを含む更新されたAPIボディで、Gaia APIコール "`set-dynamic-content`" を実行する必要があります。

  注:
  - 現在のルールを確認し、完全なJSONをコピーするには、セキュリティゲートウェイ上でGaia APIコール "`show-dynamic-layer`" を実行します。
  - 必要に応じて、セキュリティゲートウェイのダイナミックレイヤーにあるすべてのルールを削除できます。参照: *ダイナミックレイヤーのリセット (69ページ)*。

- VSNext Virtual Gatewayはサポートされていません。
- 従来のVSX Virtual System(VSX GatewayまたはVSX Cluster上) はサポートされていません。
- 従来の VSX バーチャル・ルータ(VSX ゲートウェイまたは VSX クラスタ上) はサポートされていない。

注

- 各Policy Packageはインラインレイヤーまたはオーダーレイヤーとして複数のダイナミックレイヤーをサポートする。例えば、管理者によって異なるPolicy Layersを使用することができる。
- セキュリティゲートウェイは、ポリシーパッケージ内のポリシーレイヤーの順序でアクセスコントロールルールを適用します。
- ダイナミックレイヤーで設定したルールは、セキュリティゲートウェイで初めてGaia APIコール "`set-dynamic-content`" を実行するまで適用されます。
- ポリシーパッケージから動的レイヤを削除し(または動的レイヤのチェックボックス**Set as a Dynamic Layer**をオフにし)、アクセスコントロールポリシーをインストールすると、セキュリティゲートウェイはすべての動的ルールを削除し、SmartConsoleで設定された静的ルールのみを適用します。
- SmartConsoleには、セキュリティゲートウェイで設定したダイナミックレイヤーのルールが表示されません。
- ダイナミックレイヤーでサポートされているオブジェクトのリストは、APIコール "`set-dynamic-content`" > セクション "`Request Body`" > パラメータ "`objects`" を参照してください。

設定

1. SmartConsoleでSecurity Management Server/Domain Management Serverにアクセスします。
2. 新しいPolicy Layerを追加し、Dynamic Layerとして設定します。

   注:

   - 新しいPolicy Layerは、特定のポリシーに直接設定することも、複数のポリシーの共有Policy Layerとして設定することもできます。
   - インラインレイヤ(特定のルール内)、またはオーダードレイヤ(専用のポリシーレイヤ内の個別のルールセット)を設定できます。

     参照: *オーダーレイヤーとインラインレイヤー (358ページ)*。
   - 新しいポリシーレイヤーを追加し、ダイナミックレイヤーとして設定するには、SmartConsole(後述)または管理APIコール "`add-access-layer dynamic-layer true`" (参照)を使用します(*Check Point Management API Reference* v1.8以降)。

   SmartConsoleの手順:

   特定のアクセスコントロールポリシーにレイヤーを設定するには

   a. 左上隅から、**Menu** > **Manage policies and layers**をクリックします。

   b. 左のパネルで、**Policies**をクリックします。

c. 該 当 するポリシーパッケージを右 クリックし、**Edit** アプリケーションをクリックします。

d. アクセスコント ロールセクションで、**+**アイコンをクリックします。

e. 右 上 の隅 で、**New Layer**をクリックします。

f. このポリシーレイヤーの名 前 を入 力します。

g. **General** のページで次 を行 います。

Bladesセクションで、対 応 するブレードを選 択します:

i. 必 須 : ファイアウォール

ii. オプション: アプリケーション& URLフィルタリング

h. **Advanced** のページで次 を行 います。

i. **Implicit Cleanup Action**セクションで、オプション「**Drop**」(デフォルト) を選 択します。

このDropルールは、Gaia APIコール "`set-dynamic-content`" をセキュリティゲート ウェイ上 で実 行 するまで、このOrdered Layerにマッチするすべてのトラフィックを確 実 にドロップします。

後 でSmartConsoleで変 更 できます。

ii. **Dynamic Layer**セクションで、**Set as a Dynamic Layer**を選 択します。

i. **Permissions**ページで、ダイナミックレイヤーを編 集 できる権 限 プロファイルを選 択します。これは、複 数 のダイナミックレイヤーが使 用 され、それぞれが異 なるユーザによって設 定 される場 合 に不 可 欠 です。ここに表 示 されているプロファイルだけがレイヤーを編 集 できます。レイヤーを編 集 できるプロフィールを追 加 するには、**Permissions**ページの下 に移 動します。

新 しい権 限 プロファイルを作 成 するには、SmartConsoleで、[Manage & Settings] ビュー >**Permissions & Administrators** >**Permission Profiles** を開きます。プロファイルエディターで、Access Control >**Policy** と進 み、**Edit layers by the selected profile in a layer editor** が選 択 されていることを確 認します。

j. **OK** をクリックして、**Layer Editor**ウィンドウを閉じます。

k. ポリシーのアクセスコント ロールセクションの右 側 に、**Network** (デフォルト 名) というレイヤーと新 しいダイナミックレイヤーが表 示 されます。

重 要 - これらのPolicy Layersの順 序 を変 更 することができます。

l. **OK** をクリックして、**Policy** ウィンドウを閉じます。

特 定 のルールの特 定 のアクセスコント ロールポリシーにインラインレイヤーを設 定 するには

a. 左 のナビゲーションパネルから、Security Policiesをクリックします。

b. 別 のセキュリティポリシーを開く必 要 がある場 合 :

   i. 上 部 にある [+] タブをクリックします。

   ii. 必 要 なポリシーをクリックします。

c. アクセスコント ロールセクションで、**Policy**をクリックします。

d. 該 当 するルールを探します。

e. ルールで、**Action**セルをクリック > Inline Layer をクリック > **New Layer**をクリックします。

f. このポリシーレイヤーの名 前 を入 力します。

g. **General**ページの「**Blades**」セクションで、対 応 するブレードを選 択します:

   - 必 須 : ファイアウォール
   - オプション : アプリケーション& URLフィルタリング
   - オプション : **Sharing**セクションで**Multiple policies and rules can use this layer**を選 択します。

h. **Advanced** のページで次を行います。

   i. **Implicit Cleanup Action**セクションでオプション**Accept**を選 択します。

      これにより、セキュリティゲート ウェイでGaia APIコール"`set-dynamic-content`"を実 行 するまで、このインラインレイヤーにマッチするトラフィックを必 ず受 け入 れるようになります。

      後 でSmartConsoleで変 更 できます。

   ii. **Dynamic Layer**セクションで、**Set as a Dynamic Layer**を選 択します。

i. **Permissions**ページで、ダイナミックレイヤーを編 集 できる権 限 プロファイルを選 択します。これは、複 数 のダイナミックレイヤーが使 用 され、それぞれが異 なるユーザによって設 定 される場 合 に不 可 欠 です。ここに表 示 されているプロファイルだけがレイヤーを編 集 できます。レイヤーを編 集 できるプロフィールを追 加 するには、**Permissions**ページの下 に移 動します。

   新 しい権 限 プロファイルを作 成 するには、SmartConsoleで、[Manage & Settings] ビュー >**Permissions & Administrators** >**Permission Profiles** を開きます。プロファイルエディターで、Access Control >**Policy** と進 み、**Edit layers by the selected profile in a layer editor** が選 択 されていることを確 認します。

j. **OK**をクリックして**Layer Editor** ウィンドウを閉じます。

k. ルールでは、新 しいインラインレイヤーが表 示 されています。

複 数 のアクセスコント ロールポリシーで使 用 するために、共 有 レイヤーを設 定 するには

a. 左 上 隅 から、**Menu** > **Manage policies and layers**をクリックします。

b. 左 のパネルで、レイヤー > アクセスコント ロールをクリックします。

c. 上 部 のツールバーから、**New**をクリックします。

d. このポリシーレイヤーの名 前 を入 力 します。

e. **General**ページの「**Blades**」セクションで、対 応 するブレードを選 択 します:

- 必 須 : ファイアウォール
- オプション: アプリケーション& URLフィルタリング
- オプション: **Sharing**セクションで**Multiple policies and rules can use this layer**を選 択 します。

f. **Advanced** のページで次 を行 います。

i. **Implicit Cleanup Action**セクションでオプション**Drop**を選 択 します。

このDropルールは、Gaia APIコール "`set-dynamic-content`" をセキュリティゲート ウェイ上 で実 行 するまで、このOrdered Layerにマッチするすべてのトラフィックを確 実 にドロップします。

後 でSmartConsoleで変 更 できます。

ii. **Dynamic Layer**セクションで、**Set as a Dynamic Layer**を選 択 します。

g. **Permissions**ページで、ダイナミックレイヤーを編 集 できる権 限 プロファイルを選 択 します。これは、複 数 のダイナミックレイヤーが使 用 され、それぞれが異 なるユーザによって設 定 される場 合 に不 可 欠 です。ここに表 示 されているプロファイルだけがレイヤーを編 集 できます。レイヤーを編 集 できるプロフィールを追 加 するには、**Permissions**ページの下 に移 動 します。

新 しい権 限 プロファイルを作 成 するには、SmartConsoleで、[Manage & Settings] ビュー > **Permissions & Administrators** > **Permission Profiles**を開きます。プロファイルエディタで、Access Control >**Policy** と進 み、**Edit layers by the selected profile in a layer editor** が選 択 されていることを確 認 します。

h. **OK**をクリックして、**Layer Editor**ウィンドウを閉じます。

i. 左 のパネルで、**Policies**をクリックします。

j. 該 当 するポリシーパッケージを右 クリックし、**Edit**アプリケーションをクリックします。

k. アクセスコント ロールセクションで、**+**アイコンをクリックします。

l. 新 しいダイナミックレイヤーをクリックします。

m. ポリシーのアクセスコントロールセクションの右側に、**Network**(デフォルト名)というレイヤーと新しいダイナミックレイヤーが表示されます。

重要 - これらのPolicy Layersの順序を変更することができます。

n. **OK**をクリックして、**Policy**ウィンドウを閉じます。

o. **Close**をクリックして、**Manage policies and layers**ウィンドウを閉じます。

3. リモートAPIクライアントからセキュリティゲートウェイ上でGaia APIコールを実行する場合(セキュリティゲートウェイ上でローカルに実行しない場合)、アクセスコントロールポリシーでセキュリティゲートウェイへの接続が許可されていることを確認してください。

ベストプラクティス - APIクライアントの接続損失を回避するには、該当するルールを静的 Policy Layer (Dynamic Layer として設定されていない) にのみ追加します。

4. このアクセスコントロールポリシーをセキュリティゲートウェイ / クラスタオブジェクトにインストールします。

5. セキュリティゲートウェイ/各クラスタメンバ/セキュリティグループでGaia APIコール "`set-dynamic-content`" を実行し、必要な動的アクセスコントロールルールを設定します。

警告 - セキュリティゲートウェイで設定するルールに細心の注意を払ってください。セキュリティゲートウェイで設定されたルールとSmartConsoleで設定されたルールが競合する可能性の**検証は行われません**。

注:

- オンライン*Check Point Gaia API Reference*(v1.8以降) > セクション **System** > サブセクション**Dynamic Content**。
  ローカルのGaia APIリファレンスを参照するには、Security Management Serverまたはセキュリティゲートウェイ(R82以降)でこのURLにアクセスします:

  ```
  https://<IP Address of Gaia Management Interface>/gaia_docs/#web/set-dynamic-content
  ```

  Gaia APIリファレンスの上部で、**Web Services**タブをクリックします。
- リモートAPIクライアントからGaia APIコールを実行するため、アクセスコントロールポリシーがセキュリティゲートウェイへの接続を許可していることを確認してください。

  ベストプラクティス - APIクライアントの接続損失を回避するには、該当するルールを静的アプリケーションPolicy Layer (Dynamic Layerとして設定されていない) にのみ追加します。

リモートREST APIクライアントのワークフロー(Postmanアプリケーションに基づく)

a. Postmanアプリケーションをインストールします。

b. sk143612からGaia REST APIコレクションを入手します。

c. Gaia REST APIコレクションをPostmanアプリケーションにインポートします(最初に、Postmanアカウントを作成することが重要です)。インポート方法については、Postmanのドキュメントを参照してください。

d. 必要なAPI変数を設定します:

   i. 左側のパネルで、Gaia REST APIコレクションの一番上のフォルダ**Gaia API**をクリックします。

   ii. これらの変数を追加します:

変数名	変数値	コメント
`username`	セキュリティゲートウェイ上のGaia OSで該当するユーザのユーザ名。	デフォルトのユーザは`admin`です。 他のユーザを作成することができます(**Requirements**のセクションを参照)。
`password`	セキュリティゲートウェイ上のGaia OSの該当ユーザのパスワード。	このパスワードを設定します。
`ip`	セキュリティゲートウェイ/各クラスタメンバ/セキュリティグループのGaia管理インタフェースのIPアドレス。	これは、APIクライアントが接続するセキュリティゲートウェイ/各クラスタメンバ/セキュリティグループのIPアドレスです。
`sid`	最初は空白です。	この変数は、Gaia APIコール"`login`"を実行した後に必要なSIDを格納するために使用するコンテナです。

e. ログインセッションID(SID)を取得します:

   i. 左側のペインで、フォルダ**Session Management**を開きます。

   ii. APIコール"**login**"をクリックします。

   iii. 右上の隅で、**Send**をクリックします。

   iv. 下のパネルで、パラメータ"**sid**"の値をコピーします。

f. SID変数を設定します:

i. 左側のパネルで、一番上のフォルダ「Gaia API」をクリックします。

ii. 変数**sid**のカラム**Current Value**にコピーした値を入力します。

iii. 右上の隅で、**Save**をクリックします。

g. セキュリティゲートウェイ/各クラスタメンバ/Scalable Platformセキュリティグループで APIコール"`set-dynamic-content`"を実行します:

i. 左のパネルで、API "**set-dynamic-content**" をクリックします。

ii. 上部で、**Body**タブをクリックします。

iii. 必要なパラメータと値をJSON形式で設定します。

iv. 右上の隅で、**Send**をクリックします。

v. 下のパネルで、タスクIDを持つ回答全体をコピーします。

vi. 左側のパネルで**Misc**フォルダを開き、APIコール "**show task**" をクリックします。

vii. 上部で**Body**タブをクリックし、**raw**オプションをクリックします。

viii. タスクIDを含む回答全体を貼り付けます。

ix. 右上の隅で、**Send**をクリックします。

x. 下のパネルで、APIコール"`set-dynamic-content`"のAPIレスポンスを見ます。

6. **オプション**: 設定された動的アクセスコントロールルールを調べます。

- 特定のダイナミックレイヤーに設定されたダイナミックアクセスコントロールルールを見るには、セキュリティゲートウェイ/各クラスタメンバ/セキュリティグループ上でGaia APIコール「`show-dynamic-layer`」を実行します。
- 設定されたすべてのダイナミックレイヤーで設定されたダイナミックアクセスコントロールルールを見るには、セキュリティゲートウェイ/各クラスタメンバ/セキュリティグループでGaia APIコール「`show-dynamic-layers`」を実行します。

ダイナミックレイヤーのリセット

すべての動的ルールを削除するには、セキュリティゲートウェイでこれらのルールを含む動的コンテナをリセットする必要があります。

手順

セキュリティゲートウェイ上でGaia APIコール"`set-dynamic-content`"を実行し、`"operation": "reset"`を使用します。

リモートREST APIクライアントの構 文 部 分

```
"access-layers-content": [
  {
    "name": "<Name_of_Dynamic_Layer>",
    "operation": "reset",
    "rulebase": []
  }
]
```

APIキー認証による管理者アカウントの作成

APIキーは、クライアントがAPIを呼び出す際に提供するトークンです。

APIキー認証は、管理者が通常の管理者名/パスワードの代わりにトークンを使用してAPIインタフェースを認証する機能を提供します。

管理者が管理用APIを使用するためのAPIキーをSmartConsoleで設定することができます。

注 - この管理者は、APIコマンドの実行にのみAPIを使用でき、SmartConsoleの認証には使用できません。

前提条件:

必要な権限プロファイルが設定されていることを確認してください。参照: *管理者への権限プロファイルの割り当て (116ページ)*。

SmartConsoleを使用して、管理者のAPI認証を設定する手順

1. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。。
2. **Permissions & Administrators**を展開 > **Administrators** をクリック。
3. 上部のツールバーから、アイコン (**New**) をクリック > **New Administrator** をクリック。

   New Administrator ウィンドウが開き、**General** ページが表示されます。
4. 一番上のフィールドに、該当するオブジェクト名を入力。
5. **オプション:** コメントを入力。
6. **Authentication Method**フィールドで、**API Key**を選択します。
7. **Generate API key**をクリック:
   a. クリック**Copy Key to Clipboard**
   b. キーは後で使用するために保存します(関連する管理者に提供するなど) 。
   c. クリック**OK**。
8. **Permission Profile**フィールドで、該当するプロファイルを選択します。
9. **Expiration**セクションで、必要な有効期限を設定します。
10. **オプション: Additional Info**ページで次を設定 :
    - **Phone Number**
    - **Contact Details**
    - **Email**

11. クリックOK。
12. SmartConsoleセッションを公開する。

例

この例では、APIコマンド"`login`"とAPIコマンド"`add simple-gateway`"に対してAPIキーを使用する方法を示します。

1. セキュリティ管理サーバのコマンド ラインに接続します。
2. エキスパート モードにログインします。
3. APIコマンド"`login`"を実行し、事前に生成したAPIキーを使用し、出力をファイルに保存します:

   構文:

   ```
   mgmt_cli login api-key <api-key> > /<path_to>/<filename>
   ```

   例:

   ```
   mgmt_cli login api-key mvYSiHVmlJM+J0tu2FqGag12 >
   /var/tmp/token.txt
   ```

4. APIコマンド"`add simple-gateway`"を実行します。

   `mgmt_cli`コマンドに"**-s**"フラグを付けて実行しトークンファイルを指定します。

   構文:

   ```
   mgmt_cli -s /<path_to>/<filename> add simple-gateway name
   <gateway name> ip-address <ip address> one-time-password
   <password> blade <true>
   ```

   例:

   ```
   mgmt_cli -s /var/tmp/token.txt add simple-gateway name
   "gw1" ip-address 192.168.3.181 one-time-password "aaaa"
   firewall true vpn true
   ```

   詳細 : *Check Point Management API Reference*。

API認証を設定した後、さらに証明書ファイルによる認証も設定できます。管理者は、API Keyまたは証明書ファイルのいずれかを使用して、Security Management Serverを認証できます。

SmartConsoleで証明書ファイルを作成します。管理者は証明書を使用して、SmartConsoleに2つの方法でログインできます:

- SmartConsoleに**Certificate File**オプションでログインします。証明書ファイルを使用するには、管理者がパスワードを提供する必要があります。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。管理者は、この保存された証明書を使用して、CAPI証明書オプションを使用してSmartConsoleにログインできます。管理者がログインする際にパスワードを入力する必要はありません。

管理者は、他の管理者に証明書を渡して、自分の管理者アカウントなしでSmartConsoleにログインさせることもできます。

管理者アカウントの管理

Check Pointの管理者とは、SmartConsole、CLI、またはAPIを使用してCheck Pointのセキュリティ環境を管理・保守するITプロフェッショナルのことです。Check Pointの管理者は、Check Pointのセキュリティ製品の設定と管理を行い、サイバー攻撃やマルウェアなどのセキュリティ脅威から組織のネットワークを保護します。Check Pointの管理者は通常、Check Pointソフトウェアのインストール、設定、保守、ネットワークトラフィックおよびセキュリティポリシーの管理、システムパフォーマンスのモニタリング、セキュリティ問題のトラブルシューティングなどを行います。また管理者は、Check Pointのセキュリティ環境を最新のHotfixとアップデートで更新し、最適なセキュリティを維持できるようにします。

管理者アカウントは、Check Pointの管理データベースまたは外部のLDAPサーバに保存できます。Security Management Serverは、管理者認証を行います。Check Pointは、管理者向けにさまざまな認証方法をサポートしています。

管理者として、オブジェクトやユーザの定義などのタスクを他の管理者に委任することができます。これらのタスクを実行するために必要な権限を持つ管理者アカウントを必ず作成してください。自身が唯一の管理者である場合、トラブルシューティング、コンサルテーション、または監査に便利な、読み取り専用権限を持つ2番目の管理者アカウントを作成することをお勧めします。

管理者アカウントの作成

大規模なネットワークのセキュリティを上手く管理していくためには、まず管理チームを立ち上げ、タスクを委譲することをお勧めします。

SmartConsoleの管理者アカウントは、以下の手順、または初期設定ウィザードで作成することをお勧めします。

SmartConsoleで管理者アカウントを作成する場合、これらの認証方法のいずれかを選択できます:

認証方法	説明
Check Point Password	Check Pointのパスワードは、SmartConsoleに設定されている静的なパスワードです。Security Management Serverのローカルデータベースがパスワードを保存します。追加のソフトウェアは必要ありません。 参照: *Check Pointのパスワード認証による管理者アカウントの作成 (81ページ)*。
OS Password	OSパスワードは、Security Management ServerがインストールされているコンピュータのOS上に保持されます。Windowsドメインに保存されているパスワードを使うこともできます。追加のソフトウェアは必要ありません。 参照: *OSパスワード認証による管理者アカウントの作成 (84ページ)*

認証方法	説明
RADIUS	RADIUS(Remote Authentication Dial-In User Service) は、外部認証方式の1つで、認証機能をアクセスサーバから分離することにより、セキュリティとスケーラビリティを実現するものです。RADIUSの場合、Security Management Serverは認証要求をRADIUSサーバに転送します。管理者のアカウント情報を保存しているRADIUSサーバが認証を行います。RADIUSプロトコルは、UDPを使用してセキュリティゲートウェイまたはSecurity Management Serverと通信します。 参照: *RADIUSサーバ認証による管理者アカウントの作成 (87ページ)*
TACACS	TACACS(Terminal Access Controller Access Control System) は、1つまたは複数の集中型サーバを通じて、ルータやネットワークアクセスサーバなどのネットワーク接続デバイスのアクセス制御を行うシステムです。 TACACSは、検証サービスを提供する外部認証メソッドです。TACACSでは、Security Management Serverは、リモート管理者による認証要求をTACACSサーバに転送します。管理者のアカウント情報を保存するTACACSサーバは、管理者を認証します。物理的なカードキーデバイスやトークンカード、Kerberosの秘密キー認証に対応しています。TACACSは、すべての認証要求の管理者名、パスワード、認証サービス、およびアカウンティング情報を暗号化し、通信を保護します。 参照: *TACACS サーバ認証による管理者アカウントの作成 (92ページ)*
SecurID	SecurIDは、管理者がトークン認証器を所有し、PINまたはパスワードを提供することを要求します。トークン認証は、RSA認証マネージャ(AM) に同期するワンタイムパスワードを生成するもので、ハードウェアまたはソフトウェアの形態で提供されます。ハードウェアトークンは、キーホルダーやクレジットカード大のデバイスです。ソフトウェアトークンは、管理者が認証を希望するPCやデバイスに常駐します。すべてのトークンは、約1分ごとに変化するランダムな1回限りのアクセスコードを生成します。管理者が保護されたリソースを認証しようとする場合、AMはワンタイムユースコードを検証する必要があります。 Security Management Serverは、リモート管理者によるSecurID認証要求をAMに転送します。AMは、RSAユーザおよび割り当てられたハードトークンまたはソフトトークンのデータベースを管理します。Security Management ServerはAMエージェントとして機能し、すべてのアクセス要求をRSA AMに送り認証します。エージェント設定の詳細については、RSA Authentication Managerのドキュメントを参照してください。 SecurID認証方式に必要なパラメータは特にありません。認証リクエストは、SDKがサポートするAPIまたはREST APIを介して送信できます。 参照: *SecurID認証による管理者アカウントの作成 (97ページ)*。
API Key	管理者が管理用APIを使用するためのAPIキーをSmartConsoleで設定することができます。APIを使用できるのは、APIコマンドの実行のみで、SmartConsoleの認証には使用できません。詳細 : *APIキー認証による管理者アカウントの作成 (113ページ)*

認証方法	説明
SAML	管理者は、SAMLプロトコルを使用して、中央のサードパーティIDプロバイダからSmartConsoleにログインできます。IDプロバイダは、管理者を認証する機能など、管理者に関する情報を保持します。Check Pointは、Okta、Ping Identity、AzureのIDプロバイダをサポートしています。詳細：*SAML認証ログインによる管理者アカウントの作成 (101ページ)*。

Check Pointの認証方法のいずれかを使用して認証を構成した後、さらに証明書ファイル証明書認証を構成することができます。管理者は、Check Pointの認証方式または証明書ファイルを使用して、SmartConsoleを認証します。

SmartConsoleで証明書ファイルを作成します。管理者は証明書を使用して、SmartConsoleに2つの方法でログインできます：

- SmartConsoleに**Certificate File**オプションでログインします。証明書ファイルを使用するには、管理者がパスワードを提供する必要があります。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。管理者は、この保存された証明書を使用して、CAPI証明書オプションを使用してSmartConsoleにログインできます。管理者がログインする際にパスワードを入力する必要はありません。

管理者は、他の管理者に証明書を渡して、自分の管理者アカウントなしでSmartConsoleにログインさせることもできます。

Check Point Configuration Toolツール(cpconfig) を使用して管理者アカウントを作成するには

`cpconfig`(Check Point Configuration Tool) を使用して管理者を作成することはお勧めしません。

SmartConsoleやGaia Portalにアクセスできない場合のみ使用してください。

`cpconfig`を使用して管理者を作成する場合：

- これらのコマンドを使用して管理者をアクティブにするには、Check Point Services を再起動する必要があります：

  ```
  cpstop ; cpstart
  ```

- 他の管理者は表示されません。
- 認証方法として、Check Point Passwordが自動的に設定されます。

管理者アカウントの編集

1. 左側のナビゲーションパネルでManage & Settingsをクリックします。
2. Permissions & Administratorsをクリックします。
3. 管理者アカウントをダブルクリックします。

   Administratorsプロパティウィンドウが表示されます。

管理者アカウントの削除

環境の安全性を確保するために、担当者の退職や異動時には管理者アカウントを削除することがベストプラクティスです。

管理者アカウントを削除するには

1. 左側のナビゲーションパネルでManage & Settingsをクリックします。
2. Permissions & Administratorsをクリックします。
3. 管理者アカウントを選択してDeleteをクリックします。
4. 表示される確認ウィンドウでYesをクリックします。

管理者のデフォルト有効期限

複数のアカウントで同じ有効期限を使用する場合は、管理者アカウントのデフォルトの有効期限を設定することができます。また、管理者がSmartConsoleまたはSmartConsoleクライアントのいずれかにログインしたときに、有効期限が近づいていることを通知するように選択することもできます。アカウントが生きている残りの日数は、ステータスバーに表示されます。

デフォルトの有効期限を設定するには

1. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。
2. **Permissions & Administrators** >**Advanced** をクリックします。
3. **Advanced**をクリックします。
4. **Default Expiration Date**セクションで、スナップショットを選択します。
   - **Never expires**
   - **Expire at**- カレンダーコントロールから有効期限を選択
   - **Expire after**- 管理者アカウントの有効期限が切れるまでの日数、月数、または年数(アカウントが作成された日から) を入力
5. **Expiration notifications**セクションで、**Show 'about to expire' indication in administrators view**を選択し、**days in advance**の日数を選択します。有効期限が近づいた際にメッセージが表示されます。
6. SmartConsoleセッションを公開する。

注 - 管理者に有効期限を設定した場合、管理者は自動的にログアウトされません。新規ログインのみがブロックされる。
セキュリティを向上させるには、アイドルタイムアウトを設定します。SmartConsole >**Manage & Settings** >**Permissions & Administrators** >**Advanced** >**Idle Timeout** に移動します。

SmartConsole セッションタイムアウトの設定

SmartConsoleを安全に使用し、すべての管理者に安全な使用方法を徹底します。SmartConsoleのタイムアウトを設定することは、安全に使用するための基本的な条件です。管理者がSmartConsoleを使用しない場合、ログアウトします。

SmartConsoleセッションのタイムアウトを設定するには

1. 左側のナビゲーションパネルでManage & Settingsをクリックします。
2. Permissions & Administrators >Advanced をクリックします。
3. Idle Timeout areaで、Perform logout after being idleを選択します。
4. 数を入力します(単位は分)。

   SmartConsoleがこの時間経過後にアイドル状態になると、SmartConsoleは接続している管理者を自動的にログアウトしますが、変更内容はすべて保持されます。

管理者証明書の失効

証明書によって認証される管理者が一時的に管理者の職務を果たせない場合、アカウントの証明書を取り消すことができます。管理者アカウントは残りますが、証明書を使用してSecurity Management Serverを認証することはできません。しかし、アカウントに追加の認証方法(パスワードなど)がある場合、管理者はこの方法を使用してアカウントの認証を行うことができます。

管理者証明書を失効させるには

1. 左側のナビゲーションパネルでManage & Settingsをクリックします。
2. Permissions & Administratorsをクリックします。
3. 管理者アカウントを選択してEditをクリックします。
4. General > Authenticationで、Revokeをクリックします。

管理者のログイン試行の制限

Check Pointのパスワードを使用してSecurity Management Serverにログインする管理者に対して、このようなログイン制限を設定できます:

- SmartConsoleが管理者アカウントを自動的にロックするまでのログイン試行回数。
- SmartConsoleが管理者アカウントをロックした後、ロックを解除するまでの時間(分)。

ログイン制限を設定するには

1. **Manage & Settings**ビューまたは**Multi-Domain**ビューに移動します。
2. **Permissions & Administrators** >**Advanced** >**Login Restrictions**にアクセス。

注 - これらの制限は、Check Pointのパスワードで Security Management Serverを認証する管理者 *のみ*に適用されます。

管理者アカウントのロック解除

Manage Administrators権限を持つ管理者は、ロックされている管理者がCheck Pointのパスワードでで Security Management Serverを認証した場合、他の管理者のロックを解除することができます。

管理者のロックを解除するには

1. **Manage & Settings**ビューまたは**Multi-Domain**ビューに移動します。
2. ロックされた管理者を右クリックし、**Unlock Administrator**を選択します。

または

API コマンド "unlock-administrator" を使用します。

注 - **Unlock Administrator**機能は、他の認証方法を使用している管理者には適用**されません**。

複数の管理者

2人の管理者が同じ名前の管理者アカウントを作成した場合、最初の管理者がセッションを公開すると、2番目の管理者はセッションを公開できなくなります。2人目の管理者が管理者アカウントで名前を変更しようとしてもできません。この問題を解決するには、2番目の管理者がセッションの変更を破棄し、再接続する必要があります。

Check Pointのパスワード認証による管理者アカウントの作成

Check Pointのパスワードは、SmartConsoleに設定されている静的なパスワードです。Security Management Serverのローカルデータベースがパスワードを保存します。追加のソフトウェアは必要ありません。

Check Pointのパスワードによる認証を設定した後は、証明書ファイルによる証明書認証も設定できます。管理者は、Check Pointのパスワードまたは証明書ファイルを使用してSmartConsoleを認証します。

SmartConsoleで証明書ファイルを作成します。管理者は証明書を使用して、SmartConsoleに2つの方法でログインできます:

- SmartConsoleに**Certificate File**オプションでログインします。証明書ファイルを使用するには、管理者がパスワードを提供する必要があります。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。管理者は、この保存された証明書を使用して、CAPI証明書オプションを使用してSmartConsoleにログインできます。管理者がログインする際にパスワードを入力する必要はありません。

管理者は、他の管理者に証明書を渡して、自分の管理者アカウントなしでSmartConsoleにログインさせることもできます。

前提条件:

必要な権限プロファイルが設定されていることを確認します。参照: *管理者への権限プロファイルの割り当て (116ページ)*。

Check Pointのパスワード認証を使用して新しい管理者を作成するには

1. **新しい管理者を作成し、認証方法としてCheck Pointのパスワードを定義します。**
    a. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。。
    b. **Permissions & Administrators**を展開 > **Administrators**をクリックします。
    c. 上部のツールバーから、アイコン (**New**) をクリック > **New Administrator**をクリックします。

    New Administratorウィンドウが開き、**General**ページが表示されます。
    d. 一番上のフィールドに、該当するオブジェクト名を入力します。
    e. **オプション:** コメントを入力します。
    f. **Authentication Method**フィールドで、**Check Point Password**を選択します。

g. **Set New Password**をクリックします:

   i. **Password**フィールドにパスワードを入力します。

   ii. **Confirm**フィールドで、同じパスワードを入力します。

   iii. **オプション: User must change password on next login**を選択します。

   iv. クリック**OK**。

h. **オプション:** この管理者の証明書を作成します:

   i. **Certificate Information**フィールドで、**Create**をクリックします。

   ii. **Password**フィールドにパスワードを入力します。

   パスワードは、証明書ファイル内の機密データを保護するために必要です。

   iii. **Confirm**フィールドで、同じパスワードを入力します。

   iv. クリック**OK**。

   v. **Save As**ウィンドウが開くのを待ちます。

   vi. **File name**フィールドでユーザ名を必ず入れます。

   vii. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

   証明書ファイルはPKCS #12形式で、拡張子は.p12です。

   viii. SmartConsoleコンピュータの安全な場所にアクセスします。

   ix. クリック**Save**。

   注:
   - 証明書ファイルを保存したら、管理者にこのファイルとパスワードを伝えます。
     管理者は、SmartConsoleでSecurity Management Serverにログインする際に、この証明書で認証を行うことができます。
   - この証明書はいつでも失効させることができます。証明書を選択し、**Revoke**をクリックします。

i. **Permission Profile**フィールドで、該当するプロファイルを選択します。

j. **Expiration**セクションで、必要な有効期限を設定します。

k. **オプション: Additional Info**ページで次を設定します:

   - **Phone Number**
   - **Contact Details**
   - **Email**

l. クリック**OK**。

m. SmartConsoleセッションを公開する。

2. **オプション: 証明書ファイルをWindows証明書ストアにインポート**

   注 - この手順は、管理者オブジェクトで証明書認証を作成し、CAPI証明書オプションを使用してSmartConsoleにログインする場合に適用されます。

   a. 必要な管理者を作成したときに保存した*.p12ファイルを右クリックし、**Install PFX**をクリックします。

      Certificate Import Wizardが開きます。

   b. **Store Location**セクションで、該当するオプションを選択します:

      - **Current User**(これはデフォルトです)
      - **Local Machine**

   c. **Next**をクリックします。

   d. 必要な管理者証明書を作成したときに使用したのと同じ証明書パスワードを入力します。

   e. **Enable strong private key protection**をクリアします。

   f. **Mark this key as exportable**を選択します。

   g. **Next**をクリックします。

   h. **Place all certificates in the following store**を選択し、**Browse** >**Personal** >**OK**をクリックします。

   i. **Next**をクリックします。

   j. **Finish**をクリックします。

OSパスワード認証による管理者アカウントの作成

OSパスワードは、Security Management ServerがインストールされているコンピュータのOS上に保持されます。Windowsドメインに保存されているパスワードを使うこともできます。追加のソフトウェアは必要ありません。

OSパスワードによる認証を設定した後、証明書ファイルによる認証も設定できます。管理者は、OSのパスワードまたは証明書ファイルを使ってSmartConsoleを認証することができます。

SmartConsoleで証明書ファイルを作成します。管理者は証明書を使用して、SmartConsoleに2つの方法でログインできます:

- SmartConsoleに**Certificate File**オプションでログインします。証明書ファイルを使用するには、管理者がパスワードを提供する必要があります。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。管理者は、この保存された証明書を使用して、CAPI証明書オプションを使用してSmartConsoleにログインできます。管理者がログインする際にパスワードを入力する必要はありません。

管理者は、他の管理者に証明書を渡して、自分の管理者アカウントなしでSmartConsoleにログインさせることもできます。

前提条件:

必要な権限プロファイルが設定されていることを確認してください。参照: *管理者への権限プロファイルの割り当て (116ページ)*。

管理者にCheck Pointのパスワード認証を設定するには

1. **新しい管理者を作成し、認証方法としてOSのパスワードを定義します。**
    a. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。。
    b. **Permissions & Administrators**を展開 > **Administrators**をクリックします。
    c. 上部のツールバーから、アイコン (**New**) をクリック > **New Administrator**をクリックします。

       New Administratorウィンドウが開き、**General**ページが表示されます。
    d. 一番上のフィールドに、該当するオブジェクト名を入力します。
    e. **オプション:** コメントを入力します。
    f. **Authentication Method**フィールドで、**OS Password**を選択します。

g. **オプション:** この管理者の証明書を作成します:

i. **Certificate Information**フィールドで、**Create**をクリックします。

ii. **Password**フィールドにパスワードを入力します。

パスワードは、証明書ファイル内の機密データを保護するために必要です。

iii. **Confirm**フィールドで、同じパスワードを入力します。

iv. クリック**OK**。

v. **Save As**ウィンドウが開くのを待ちます。

vi. **File name**フィールドで、ユーザ名を必ず入れます。

vii. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

証明書ファイルはPKCS #12形式で、拡張子は`.p12`です。

viii. SmartConsoleコンピュータの安全な場所にアクセスします。

ix. クリック**Save**。

注:

- 証明書ファイルを保存したら、管理者にこのファイルとパスワードを渡します。
  管理者は、SmartConsoleでSecurity Management Serverにログインする際に、この証明書で認証を行うことができます。
- この証明書はいつでも失効させることができます。証明書を選択し、**Revoke**をクリックします。

h. **Permission Profile**フィールドで、該当するプロファイルを選択します。

i. **Expiration**セクションで、必要な有効期限を設定します。

j. **オプション: Additional Info**ページで設定します:

- **Phone Number**
- **Contact Details**
- **Email**

k. クリック**OK**。

l. SmartConsoleセッションを公開する。

2. **オプション: 証明書ファイルをWindows証明書ストアにインポート**

注 - この手順は、管理者オブジェクトで証明書認証を作成し、CAPI証明書オプションを使用してSmartConsoleにログインする場合に適用されます。

a. 必要な管理者を作成したときに保存した*.p12ファイルを右クリックし、**Install PFX**をクリックします。

   Certificate Import Wizardが開きます。

b. **Store Location**セクションで、該当するオプションを選択します:

   - **Current User**(これはデフォルトです)
   - **Local Machine**

c. **Next**をクリックします。

d. 必要な管理者証明書を作成したときに使用したのと同じ証明書パスワードを入力します。

e. **Enable strong private key protection**をクリアします。

f. **Mark this key as exportable**を選択します。

g. **Next**をクリックします。

h. **Place all certificates in the following store**を選択し、**Browse** >**Personal** >**OK**をクリックします。

i. **Next**をクリックします。

j. **Finish**をクリックします。

RADIUSサーバ認証による管理者アカウントの作成

RADIUS(Remote Authentication Dial-In User Service) は、外部認証方式の1つで、認証機能をアクセスサーバから分離することにより、セキュリティとスケーラビリティを実現するものです。RADIUSの場合、Security Management Serverは認証要求をRADIUSサーバに転送します。管理者のアカウント情報を保存しているRADIUSサーバが認証を行います。RADIUSプロトコルは、UDPを使用してセキュリティゲートウェイまたはSecurity Management Serverと通信します。

SmartConsoleの管理者のRADIUS認証は、RADIUSサーバまたはRADIUSサーバグループを通して行うことができます。SmartConsoleでRADIUSサーバとRADIUSサーバグループオブジェクトを定義します。RADIUSサーバグループは、同一のRADIUSサーバからなるハイアベイラビリティなグループであり、システム内の任意またはすべてのRADIUSサーバが含まれます。グループを作成する際に、グループ内の各サーバに優先順位を定義します。優先順位の高いサーバに障害が発生すると、グループ内で次に優先順位の高いサーバに引き継がれ、その後も同様になります。すべてのRADIUSサーバに同じ優先順位を割り当てると、セキュリティゲートウェイはそのうちの1つをランダムに選択して認証を行います。RADIUSサーバのグループを定義する場合、グループのすべてのメンバは同じプロトコルを使用する必要があります。

RADIUSサーバの設定方法については、ベンダーのドキュメントを参照してください。

RADIUSサーバ認証を設定した後、さらに、証明書ファイルによる認証を設定することができます。管理者は、RADIUSサーバまたは証明書ファイルを使用してSmartConsoleを認証できます。

SmartConsoleで証明書ファイルを作成します。管理者は証明書を使用して、SmartConsoleに2つの方法でログインできます:

- SmartConsoleに**Certificate File**オプションでログインします。証明書ファイルを使用するには、管理者がパスワードを提供する必要があります。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。管理者は、この保存された証明書を使用して、CAPI証明書オプションを使用してSmartConsoleにログインできます。管理者がログインする際にパスワードを入力する必要はありません。

管理者は、他の管理者に証明書を渡して、自分の管理者アカウントなしでSmartConsoleにログインさせることもできます。

前提条件:

必要な権限プロファイルが設定されていることを確認してください。参照: *管理者への権限プロファイルの割り当て (116ページ)*。

管理者のRADIUSサーバ認証を設定するには

1. **SmartConsoleで、新しいRADIUSサーバオブジェクトを設定します。**

    a. オブジェクトエクスプローラーを開き、**New** >**More** >**Server** > RADIUSを選択します。

    b. サーバに**Name**を指定します。任意の名前を選択できます。

    c. **Host**フィールドで、ドロップダウン矢印をクリックし、**New**をクリックして、RADIUSサーバの**New Host**で**IP address**を作成します。

    d. クリック**OK**。

    このホストが、**New RADIUS**ウィンドウの**Host**フィールドに表示されるようになりました。

    e. **Shared Secret**フィールドに、以前にRADIUSサーバで定義した秘密キーを入力します。

    f. クリック**OK**。

    g. SmartConsoleセッションを公開する。

2. **新しい管理者を作成し、認証方法としてRADIUSを定義します。**

    a. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。。

    b. **Permissions & Administrators**を展開 > **Administrators**をクリックします。

    c. 上部のツールバーから、アイコン (**New**) をクリック > **New Administrator**をクリックします。

    New Administratorウィンドウが開き、**General**ページが表示されます。

    d. 一番上のフィールドに、RADIUSサーバで設定したユーザ名を入力します。

    e. **オプション:** コメントを入力します。

    f. **Authentication Method**フィールドで**RADIUS**を選択します。

    g. **RADIUS Server**フィールドで、先ほど設定したRADIUSサーバオブジェクトを選択します。

h. **オプション:** この管理者の証明書を作成します:

i. **Certificate Information**フィールドで、**Create**をクリックします。

ii. **Password**フィールドにパスワードを入力します。

パスワードは、証明書ファイル内の機密データを保護するために必要です。

iii. **Confirm**フィールドで、同じパスワードを入力します。

iv. クリック**OK**。

v. **Save As**ウィンドウが開くのを待ちます。

vi. **File name**フィールドでユーザ名を必ず入れます。

vii. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

証明書ファイルはPKCS #12形式で、拡張子は`.p12`です。

viii. SmartConsoleコンピュータの安全な場所にアクセスします。

ix. クリック**Save**。

注:

- 証明書ファイルを保存したら、管理者にこのファイルとパスワードを渡します。
  管理者は、SmartConsoleでSecurity Management Serverにログインする際に、この証明書で認証を行うことができます。
- この証明書はいつでも失効させることができます。証明書を選択し、**Revoke**をクリックします。

i. **Permission Profile**フィールドで、該当するプロファイルを選択します。

j. **Expiration**セクションで、必要な有効期限を設定します。

k. **オプション:** **Additional Info**ページで次を設定します:

- **Phone Number**
- **Contact Details**
- **Email**

l. クリック**OK**。

m. SmartConsoleセッションを公開する。

3. **オプション: SmartConsole管理者認証用のRADIUSサーバグループを設定します。**

a. SmartConsoleで、以下の説明に従って、サーバグループに含めるすべてのサーバを設定します。*管理者のRADIUSサーバ認証を設定するには (88ページ)*。

   各サーバについて、グループ内の優先順位を入力します。数字が小さいほど優先順位が高くなります。

   たとえば、優先度1、2、3の3台のサーバでグループを作成した場合、1番のサーバが1番目に、2番のサーバが2番目に、3番のサーバが3番目にアプローチされます。

b. サーバグループを作成します。

   SmartConsole のオブジェクトエクスプローラで、**New** > **Server** > **More** > **RADIUS Group**をクリックします。

c. グループのプロパティを設定し、サーバをグループに追加します。

   i. グループに**Name**を付けます。任意の名前を選択できます。

   ii. 追加する各サーバの**+**アイコンをクリックし、ドロップダウンリストからサーバを選択します。

   iii. クリック**OK**。

   iv. SmartConsoleセッションを公開する。

4. **オプション: 証明書ファイルをWindows証明書ストアにインポート**

   注 - この手順は、管理者オブジェクトで証明書認証を作成し、CAPI証明書オプションを使用してSmartConsoleにログインする場合に適用されます。

   a. 必要な管理者を作成したときに保存した*.p12ファイルを右クリックし、**Install PFX**をクリックします。

      Certificate Import Wizardが開きます。

   b. **Store Location**セクションで、該当するオプションを選択します:

      - **Current User**(これはデフォルトです)
      - **Local Machine**

   c. **Next**をクリックします。

   d. 必要な管理者証明書を作成したときに使用したのと同じ証明書パスワードを入力します。

   e. **Enable strong private key protection**をクリアします。

   f. **Mark this key as exportable**を選択します。

   g. **Next**をクリックします。

h. **Place all certificates in the following store**を選択し、**Browse** >**Personal** >**OK**をクリックします。

i. **Next**をクリックします。

j. **Finish**をクリックします。

TACACS サーバ認証による管理者アカウントの作成

TACACS(Terminal Access Controller Access Control System) は、1つまたは複数の集中型サーバを通じて、ルータやネットワークアクセスサーバなどのネットワーク接続デバイスのアクセス制御を行うシステムです。

TACACSは、検証サービスを提供する外部認証メソッドです。TACACSでは、Security Management Serverは、リモート管理者による認証要求をTACACSサーバに転送します。管理者のアカウント情報を保存するTACACSサーバは、管理者を認証します。物理的なカードキーデバイスやトークンカード、Kerberosの秘密キー認証に対応しています。TACACSは、すべての認証要求の管理者名、パスワード、認証サービス、およびアカウンティング情報を暗号化し、通信を保護します。

SmartConsoleの管理者のTACACS認証は、TACACSサーバまたはTACACSサーバグループを通して行うことができます。TACACSサーバグループは、システム内の同一のTACACSサーバからなるハイアベイラビリティグループです。グループを作成する際に、各サーバの優先順位を定義します。優先順位の高いサーバに障害が発生すると、グループ内で次に優先順位の高いサーバに引き継がれ、その後も同様になります。すべての TACACS サーバに同じ優先度を割り当てると、セキュリティゲートウェイは認証のためにそのうちの 1 つをランダムに選択します。グループ内のすべてのTACACSサーバは、同じプロトコルを使用しなければなりません。

TACACSサーバの設定方法については、ベンダーのドキュメントを参照してください。

TACACSサーバ認証を構成した後、さらに、証明書ファイルによる認証も設定できます。管理者は、TACACSサーバまたは証明書ファイルを使用してSmartConsoleを認証できます。

SmartConsoleで証明書ファイルを作成します。管理者は証明書を使用して、SmartConsoleに2つの方法でログインできます:

- SmartConsoleに**Certificate File**オプションでログインします。証明書ファイルを使用するには、管理者がパスワードを提供する必要があります。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。管理者は、この保存された証明書を使用して、CAPI証明書オプションを使用してSmartConsoleにログインできます。管理者がログインする際にパスワードを入力する必要はありません。

管理者は、他の管理者に証明書を渡して、自分の管理者アカウントなしでSmartConsoleにログインさせることもできます。

前提条件:

必要な権限プロファイルが設定されていることを確認してください。参照: *管理者への権限プロファイルの割り当て (116ページ)*。

管理者のTACACSサーバ認証を設定する手順

1. **SmartConsoleで、新しいTACACSサーバオブジェクトを追加します。**

    a. オブジェクトエクスプローラに移動し、**New** >**More** >**Server** > TACACSをクリックします。

    b. サーバの**Name**を入力します。

    c. **Host**フィールドで、ドロップダウン矢印をクリックし、**New**をクリックしてTACACS サーバの**IP address**で**New Host**を作成します。

    d. クリック**OK**。

    このホストが、**New TACACS**ウィンドウの**Host**フィールドに表示されるようになりました。

    e. **Server type**を選択します。

    f. サーバのタイプがTACACS+の場合、TACACS+サーバで以前に定義した**Secret key**を入力します。

    g. クリック**OK**。

    h. SmartConsoleセッションを公開する。

2. **新しい管理者を追加し、認証方法を定義します。**

    a. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。。

    b. **Permissions & Administrators**を展開 > **Administrators**をクリックします。

    c. 上部のツールバーから、アイコン (**New**) をクリック >**New Administrator** をクリックします。

    New Administratorウィンドウが開き、**General**ページが表示されます。

    d. 一番上のフィールドに、TACACSサーバで設定したユーザ名を入力します。

    e. **オプション:** コメントを入力します。

    f. **Authentication Method**フィールドで、**TACACS**を選択します。

    g. **TACACS Server**フィールドで、先ほど設定したTACACSサーバオブジェクトを選択します。

h. **オプション:** この管理者の証明書を作成します:

i. **Certificate Information**フィールドで、**Create**をクリックします。

ii. **Password**フィールドにパスワードを入力します。

パスワードは、証明書ファイル内の機密データを保護するために必要です。

iii. **Confirm**フィールドで、同じパスワードを入力します。

iv. クリック**OK**。

v. **Save As**ウィンドウが開くのを待ちます。

vi. **File name**フィールドに、ユーザ名を必ず入れます。

vii. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

証明書ファイルはPKCS #12 形式で、拡張子は.p12です。

viii. SmartConsoleコンピュータの安全な場所にアクセスします。

ix. クリック**Save**。

注:

- 証明書ファイルを保存したら、管理者にこのファイルとパスワードを渡します。
  管理者は、SmartConsoleでSecurity Management Serverにログインする際に、この証明書で認証を行うことができます。
- この証明書はいつでも失効させることができます。証明書を選択し、**Revoke**をクリックします。

i. **Permission Profile**フィールドで、該当するプロファイルを選択します。

j. **Expiration**セクションで、必要な有効期限を設定します。

k. **オプション:** **Additional Info**ページで次を設定します:

- **Phone Number**
- **Contact Details**
- **Email**

l. クリック**OK**。

m. SmartConsoleセッションを公開する。

3. **オプション: SmartConsoleの管理者認証用にTACACSサーバグループを設定します。**

a. SmartConsoleで、以下の説明に従って、サーバグループに含めるすべてのサーバを設定します。*管理者のTACACSサーバ認証を設定する手順 (93ページ)*。

   各サーバについて、グループ内の優先順位を入力します。数字が小さいほど優先順位が高くなります。

   たとえば、優先度1、2、3の3台のサーバでグループを作成した場合、1番のサーバが1番目に、2番のサーバが2番目に、3番のサーバが3番目にアプローチされます。

b. サーバグループを作成します。

   SmartConsoleのオブジェクトエクスプローラーで、**New >Server >More >TACACS Group** をクリックします。

c. グループのプロパティを設定し、サーバをグループに追加します。

   i. グループの**Name**を入力します。

   ii. 追加する各サーバの**+**アイコンをクリックし、ドロップダウンリスト からサーバを選択します。

   iii. クリック**OK**。

   iv. SmartConsoleセッションを公開する。

4. **オプション: 証明書ファイルをWindows証明書ストアにインポート**

   注 - この手順は、管理者オブジェクトで証明書認証を作成し、CAPI証明書オプションを使用してSmartConsoleにログインする場合に適用されます。

   a. 必要な管理者を作成したときに保存した*.p12ファイルを右クリックし、**Install PFX** をクリックします。

      Certificate Import Wizardが開きます。

   b. **Store Location**セクションで、該当するオプションを選択します:

      - **Current User**(これはデフォルトです)
      - **Local Machine**

   c. **Next**をクリックします。

   d. 必要な管理者証明書を作成したときに使用したのと同じ証明書パスワードを入力します。

   e. **Enable strong private key protection**をクリアします。

   f. **Mark this key as exportable**を選択します。

   g. **Next**をクリックします。

h. **Place all certificates in the following store**を選択し、**Browse** >**Personal** >**OK**をクリックします。

i. **Next**をクリックします。

j. **Finish**をクリックします。

SecurID認証による管理者アカウントの作成

SecurIDは、管理者がトークン認証器を所有し、PINまたはパスワードを提供することを要求します。トークン認証は、RSA認証マネージャ(AM) に同期するワンタイムパスワードを生成するもので、ハードウェアまたはソフトウェアの形態で提供されます。ハードウェアトークンは、キーホルダーやクレジットカード大のデバイスです。ソフトウェアトークンは、管理者が認証を希望するPCやデバイスに常駐します。すべてのトークンは、約1分ごとに変化するランダムな1回限りのアクセスコードを生成します。管理者が保護されたリソースを認証しようとする場合、AMはワンタイムユースコードを検証する必要があります。

Security Management Serverは、リモート管理者によるSecurID認証要求をAMに転送します。AMは、RSAユーザおよび割り当てられたハードトークンまたはソフトトークンのデータベースを管理します。Security Management ServerはAMエージェントとして機能し、すべてのアクセス要求をRSA AMに送り認証します。エージェント設定の詳細については、RSA Authentication Managerのドキュメントを参照してください。

SecurID認証方式に必要なパラメータは特にありません。認証リクエストは、SDKがサポートするAPIまたはREST APIを介して送信できます。

SecurIDサーバの設定方法については、ベンダーのドキュメントを参照してください。

SecurID認証を設定した後、さらに証明書ファイルによる認証も設定できます。管理者は、SecurID認証または証明書ファイルを使用してSmartConsoleを認証できます。

SmartConsoleで証明書ファイルを作成します。管理者は証明書を使用して、SmartConsoleに2つの方法でログインできます:

- SmartConsoleに**Certificate File**オプションでログインします。証明書ファイルを使用するには、管理者がパスワードを提供する必要があります。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。管理者は、この保存された証明書を使用して、CAPI証明書オプションを使用してSmartConsoleにログインできます。管理者がログインする際にパスワードを入力する必要はありません。

管理者は、他の管理者に証明書を渡して、自分の管理者アカウントなしでSmartConsoleにログインさせることもできます。

前提条件:

必要な権限プロファイルが設定されていることを確認してください。参照: *管理者への権限プロファイルの割り当て (116ページ)*。

管理者のSecurID認証を設定するには

1. **SecurIDを使用するようにSecurity Management Serverを設定します(この手順は、SDKがサポートするAPIを使用する場合にのみ関連します。)**

a. セキュリティ管理サーバのコマンド ラインに接続します。

b. エキスパートモードにログインします。

c. `sdconf.rec`ファイルを`/var/ace/`ディレクトリにコピーします。

`/var/ace/`ディレクトリが存在しない場合は、このコマンドで作成します。

```
mkdir -v /var/ace/
```

d. `sdconf.rec`ファイルにすべての権限を割り当てます。

```
chmod -v 777 /var/ace/sdconf.rec
```

2. **SecurIDサーバオブジェクトの設定**

a. 新しいSecurIDサーバオブジェクトを追加します:

オブジェクト エクスプローラに移動し、**New** >**More** >**Server** >**New SecurID** を選択します。

b. 一番上のフィールドに、該当するオブジェクト名を入力します。

c. **オプション:** コメントを入力します。

d. このステップはSDKがサポートするAPIにのみ適用されます:

Browseをクリックし、`sdconf.rec`ファイルを選択します。

これは、Security Management Serverにあるファイルのコピーでなければなりません。

e. クリック**OK**。

3. **新しい管理者を追加し、認証方法としてSecurIDを定義します。**

a. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。。

b. **Permissions & Administrators**を展開 > **Administrators**をクリックします。

c. 上部のツールバーから、アイコン (**New**) をクリック > **New Administrator**をクリックします。

New Administratorウィンドウが開き、**General**ページが表示されます。

d. 一番上のフィールドに、該当するオブジェクト名を入力します。

e. **オプション:** コメントを入力します。

f. **Authentication method**で、**SecurID**を選択します。

g. **オプション:** この管理者の証明書を作成します:

i. **Certificate Information**フィールドで、**Create**をクリックします。

ii. **Password**フィールドにパスワードを入力します。

パスワードは、証明書ファイル内の機密データを保護するために必要です。

iii. **Confirm**フィールドで、同じパスワードを入力します。

iv. クリック**OK**。

v. **Save As**ウィンドウが開くのを待ちます。

vi. **File name**フィールドで、ユーザ名を必ず入れます。

vii. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

証明書ファイルはPKCS #12形式で、拡張子は.p12です。

viii. SmartConsoleコンピュータの安全な場所にアクセスします。

ix. クリック**Save**。

注:

- 証明書ファイルを保存したら、管理者にこのファイルとパスワードを渡します。
  管理者は、SmartConsoleでSecurity Management Serverにログインする際に、この証明書で認証を行うことができます。
- この証明書はいつでも失効させることができます。証明書を選択し、**Revoke**をクリックします。

h. **Permission Profile**フィールドで、該当するプロファイルを選択します。

i. **Expiration**セクションで、必要な有効期限を設定します。

j. **オプション: Additional Info**ページで次を設定します:

- **Phone Number**
- **Contact Details**
- **Email**

k. クリック**OK**。

l. SmartConsoleセッションを公開する。

4. **オプション: 証明書ファイルをWindows証明書ストアにインポート**

注 - この手順は、管理者オブジェクトで証明書認証を作成し、CAPI証明書オプションを使用してSmartConsoleにログインする場合に適用されます。

a. 必要な管理者を作成したときに保存した*.p12ファイルを右クリックし、**Install PFX**をクリックします。

   Certificate Import Wizardが開きます。

b. **Store Location**セクションで、該当するオプションを選択します:

   - **Current User**(これはデフォルトです)
   - **Local Machine**

c. **Next**をクリックします。

d. 必要な管理者証明書を作成したときに使用したのと同じ証明書パスワードを入力します。

e. **Enable strong private key protection**をクリアします。

f. **Mark this key as exportable**を選択します。

g. **Next**をクリックします。

h. **Place all certificates in the following store**を選択し、**Browse** >**Personal** >**OK**をクリックします。

i. **Next**をクリックします。

j. **Finish**をクリックします。

SAML認証ログインによる管理者アカウントの作成

SAML認証を使用すると、管理者は、SAMLプロトコルを使用する中央のサードパーティIDプロバイダを介してSmartConsoleにログインします。IDプロバイダは、管理者を認証する機能など、管理者に関する情報を保持します。Check Pointでは、Okta、Ping Identity、AzureのIDプロバイダをサポートしています。

使用事例

Azureのアカウントを持つ管理者は、SmartConsoleで作業できれば効率的です。各管理者が、Azure用とSmartConsole用の2つの異なる管理者名とパスワードを使用すると、多くの問題が発生します:

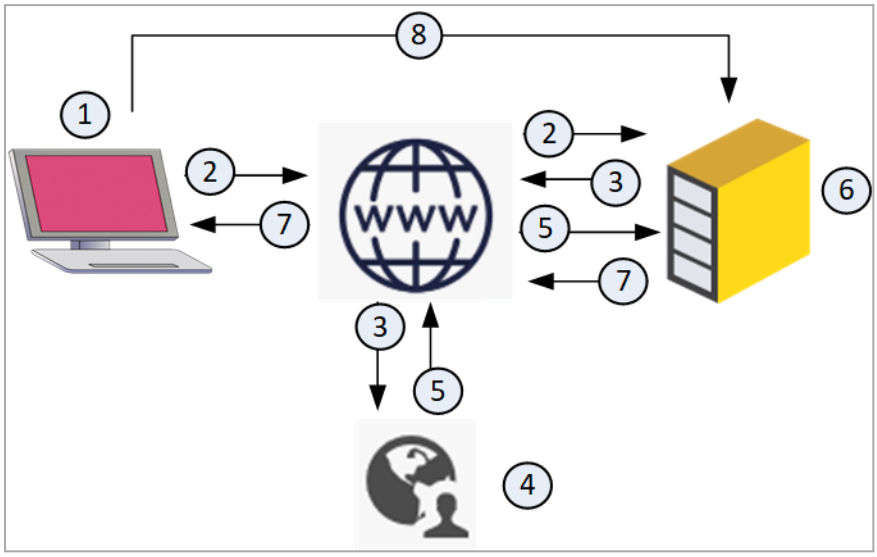
- 管理者は、(他の企業パスワードに加えて) 別のパスワードと有効期限ポリシーを扱わなければならない。
- Azure用とSmartConsole用の2つの異なるパスワードを覚えておく必要がある(他の企業パスワードに加えて) 。
- 管理者のメンテナンスが必要になる。例えば、管理者が退社する際、登録しているすべてのアプリケーションから削除する必要がある。Identity Providerを使用する場合は、Identity Providerデータベースから管理者を削除するだけです。

つまり、各管理者はAzureとSmartConsoleの両方で1つのパスワードを使用することが望ましいと言えます。IDプロバイダを使用すると、管理者はAzureに対して一度認証を行うだけで、SmartConsoleに接続したときにSmartConsoleがすでに管理者を認識しているため、改めてパスワードを入力する必要がありません。管理者もSecurity Management Serverにパスワードを知られることはありません。

SAML 認証プロセスフロー:

1. 管理者がSmartConsoleにログインしようとします。
2. SmartConsoleは、管理者をブラウザに戻し、Security Management Serverで事前に設定されたURLにリダイレクトします。
3. Security Management Serverにより、SAMLリクエストでブラウザからIDプロバイダにリダイレクトされます。
4. IDプロバイダが管理者を認証します。
5. IDプロバイダはSAMLアサーションを生成し、ブラウザを介してSecurity Management Serverに送り返します。
6. Security Management ServerでSAMLアサーションを検証します。
7. 管理者が認証されている場合、Security Management Serverは、認証に必要なデータをブラウザからSmartConsoleにリダイレクトします。

8. SmartConsoleは、この認証データでSecurity Management Serverへのセッションを開きます。



SAML認証ログイン

注 - デフォルトでは、SmartConsoleログイン用のSAML認証は、管理サーバ上のGaia PortalがTCPポート443で動作する必要があります。Gaia Portalが別のポートで動作している場合は、SmartConsoleのログインウィンドウ(`<IP_Address>:<Port>`)にそのポート番号を入力してください。詳細は、sk182032を参照してください。

1. **IDプロバイダで、SmartConsoleアプリケーションを作成し、その設定を行います。**

   手順については、IDプロバイダのマニュアルを参照してください。

   注:
   - クライアントがIDプロバイダのWebサイトに接続でき、それをブロックするポリシールールがないことを確認します。
   - IDプロバイダのSmartConsoleアプリケーション統合には、「username」の属性マッピングが必要であり、「sign assertion and response」オプションが選択されている必要があります。
   - IDプロバイダは複数のURLに応答を返すことができます。Management High Availability環境では、必要な数の返信URLを入力します。
     IDプロバイダが応答を送信するとき、応答には応答が返されるIPアドレスを含める必要があります。
     必要な宛先が応答に含まれていない場合、その応答は排除されます。
     返信URLに"Default"を使用しないでください:



2. **SmartConsoleで、Identity Providerオブジェクトを作成し、その設定を行います。**

a. オブジェクトエクスプローラで、**New** > **More** > **User/Identity** > Identity Providerをクリックします。

New Identity Providerウィンドウが開きます。

b. これらのプロパティをIDプロバイダオブジェクトに設定します:

- 名前(例:Azure)。
- **Use Identity Provider for- Managing administrator access**を選択します。IDプロバイダを通してSmartConsoleの認証を行います。

  注 - Security Gateway and logsでSAML認証を使用するには、以下を参照してください。*R82 Identity Awareness Administration Guide*。

- **Data Required by the SAML Identity Provider**- SmartConsoleは環境に応じて**Identifier (Entity ID)**、**Reply URLs**を作成します。

  SmartConsoleが示した識別子(エンティティID)と返信URLを取得し、IDプロバイダで作成したSmartConsoleアプリケーションのプロパティの該当する場所に入力します。

  URLの代わりにドメイン名を使用するには

  注 - NAT背後にあるSecurity Management ServerとMulti-Domain Serverの場合は、以下の手順に従います。

  Management High Availability環境では、各管理サーバで以下の手順を実行する必要があります。

  i. 管理サーバのコマンドラインに接続します。

  ii. エキスパートモードにログインします。

  iii. 現在の`$CPDIR/tmp/.CPprofile.sh`ファイルをバックアップします。

  ```
  cp -v$CPDIR/tmp/.CPprofile.sh{,_BKP}
  ```

  iv. `$CPDIR/tmp/.CPprofile.sh`ファイルを編集します。

  ```
  vi $CPDIR/tmp/.CPprofile.sh
  ```

  v. ファイルの一番下に次の行を追加します:

  ```
  SAML_IP_OR_NAME=<Your Domain Name>;export
  SAML_IP_OR_NAME
  ```

  例:

  ```
  SAML_IP_OR_NAME=example.com;export SAML_IP_
  OR_NAME
  ```

  vi. 変更内容をファイルに保存し、エディタを終了します。

vii. Check Pointのサービスを再起動します(この操作でSmartConsoleクライアントは切断されます) :

- Security Management Serverで、以下を実行:`cpstop ; cpstart`
- マルチドメインサーバで次を実行します:`mdsstop ; mdsstart`

viii. SmartConsoleで管理サーバに接続します。

ix. Identity Provider Web サイトを開きます。

x. **Reply URLs**で、IPアドレスをドメイン名に置き換えます。

- **Data received from the SAML Identity Provider**:
  - **Import metadata file**- IDプロバイダはこのファイルを作成します。メタデータファイルには、IDプロバイダと管理サーバ間の信頼確立に必要なすべての情報が含まれます。
  - IDプロバイダにメタデータファイルがない場合は、IDプロバイダのこの情報を手動で入力します:
    - **Identifier (Entity ID)**- IDプロバイダの一意の識別子。
    - **Login (URL)**- これはSAMLリクエストがポストされるIDプロバイダ側のエンドポイントです。
    - **Certificate file**- 管理サーバはIDプロバイダから証明書ファイルを受け取り、IDプロバイダのシグネチャを検証します。証明書は管理サーバに保存され、応答が投稿されるたびに使用されます。

c. クリック**OK**。

d. SmartConsoleセッションを公開する。

3. SmartConsoleで、Manage & Settingsビュー > **Permissions & Administrators** > **Advanced** > IDプロバイダ > **Identity Provider for Managing Administrator Access** > 作成したIdentity Providerオブジェクトを選択します。

注

- Security Management Serverでは、1つのIDプロバイダしか使用できません。
- Multi-Domain Security Management Server:
  - ドメインに使用できるIDプロバイダは1つだけです。
  - Multi-Domain ServerにIDプロバイダを構成し、ドメインにIDプロバイダを構成しない場合、ドメイン管理サーバではMulti-Domain Serverに構成されたIDプロバイダを使用します。
  - ドメインにIDプロバイダを割り当てることができるのは、スーパーユーザのみです。
  - ドメインのIDプロバイダでドメインにアクセスするには、SmartConsoleを開き、ドメインのIPアドレスに接続します。
  - ドメインのIDプロバイダは、ドメインの権限プロファイルを持つ管理者またはグループのみを認証できます。

4. **IDプロバイダと認証する管理者(または管理者のグループ)を作成します。**

   前提条件:必要な権限プロファイルが設定されていることを確認します。参照:*管理者への権限プロファイルの割り当て(116ページ)*。

   a. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。。

   b. **Permissions & Administrators**を展開 > **Administrators** をクリックします。

   c. 上部のツールバーから、アイコン (**New**) をクリック > **New Administrator**をクリックします。

      New Administratorウィンドウが開き、**General**ページが表示されます。

   d. 一番上のフィールドに、該当するオブジェクト名を入力します。

      オブジェクト名は、IDプロバイダのusername属性で定義されている名前と同じにします。

   e. **オプション:**コメントを入力します。

   f. **Authentication Method**フィールドで、**Identity Provider**を選択します。

g. **オプション:** この管理者の証明書を作成します:

   i. **Certificate Information**フィールドで、**Create**をクリックします。

   ii. **Password**フィールドでパスワードを入力します。

   パスワードは、証明書ファイル内の機密データを保護するために必要です。

   iii. **Confirm**フィールドで同じパスワードを入力します。

   iv. クリック**OK**。

   v. **Save As**ウィンドウが開くのを待ちます。

   vi. **File name**フィールドでユーザ名を必ず入力します。

   vii. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

   証明書ファイルはPKCS #12形式で、拡張子は.p12です。

   viii. SmartConsoleコンピュータの安全な場所にアクセスします。

   ix. クリック**Save**。

   注:
   - 証明書ファイルを保存したら、管理者にこのファイルとパスワードを渡します。
     管理者は、SmartConsoleでSecurity Management Serverにログインする際に、この証明書で認証を行うことができます。
   - この証明書はいつでも失効させることができます。証明書を選択し、**Revoke**をクリックします。

h. **Permission Profile**フィールドで、該当するプロファイルを選択します。

i. **オプション: Additional Info**ページで次を設定します:

   - **Phone Number**
   - **Contact Details**
   - **Email**

j. クリック**OK**。

k. SmartConsoleセッションを公開する。

注：

- IDプロバイダのインタフェースで、SAML属性を構成する：
  i. `groups`というオプションの属性を定義します。
  ii. IDプロバイダの要件に従って属性を構成します。
- 管理者グループを構成する場合は、以下の設定を行います。
  - **Name**- 管理者グループオブジェクトの名前を入力します。任意の名前を選択できます。
  - **Group ID/name**- IDプロバイダで定義されているグループ属性と同一にします。
- **Expiration**の日付は、IDプロバイダのデータベースで定義されているため、グレイアウトされます。

5. IDプロバイダを使用してSmartConsoleにログインする方法は2つあります。

   SmartConsoleのログインウィンドウからログイン

   a. SmartConsoleを開きます。

   b. 最初のドロップダウンメニューから、**Identity Provider**を選択します。

      Security Management Serverで、管理者がSecurity Management Serverのデータベースに存在するかどうかを確認します。

      - 管理者が存在する場合、SmartConsoleは管理者をログインさせます。
      - 管理者が存在しない場合、Security Management Serverで、管理者がSecurity Management Serverデータベースの管理者グループに属しているかどうかを確認します。

        このようなグループに管理者が存在する場合、SmartConsoleは管理者にログインし、Security Management Serverは管理者にグループの権限を割り当てます。

   c. 管理サーバのIPアドレスまたはホスト名を入力します。

   d. **Login with SSO**をクリックします。

注：

- 管理者が管理者アカウントを持ち、かつ管理者グループに属している場合、Security Management Serverは管理者に管理者アカウントの権限を割り当てます。
- 管理者が複数の管理者グループに属している場合、Security Management Serverは、Security Management Serverデータベースのアルファベット順で最初に来る管理者グループの権限を管理者に割り当てます。
- Security Management Serverセッションがアクティブな間に、IDプロバイダで管理者オブジェクトを切断または**編集しても**、管理者セッションは切断されません。

ベストプラクティス - IDプロバイダが利用できない場合に備えて、IDプロバイダを通じて認証されない管理者を最低1人使用することを推奨します。

SmartConsole設定ファイルによるログイン

CLI構文:

SAMLログイン用の構成ファイルを使用してSmartConsoleを起動するには、Windowsコマンドプロンプトで次のコマンドを使用します:

```
SmartConsole.exe -p "Full Path to the Configuration File"
```

例:

```
cd /d "C:\Program Files (x86)\CheckPoint\SmartConsole\R82\"
SmartConsole.exe -p "D:\MySAML_Configuration.xml"
```

必要な設定ファイル:

これは必要な設定ファイル(プレーンテキストのXML)です:

```
<?xml version="1.0" encoding="utf-8"?>
<RemoteLaunchParemeters
xmlns:xsi="http:/www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http:/www.w3.org/2001/XMLSchema">
  <ServerIP>IP Address of the Management Server</ServerIP>
  <DomainName>Name of the Domain Management Server</DomainName>
  <ReadOnly>False</ReadOnly>
  <CloudDemoMode>False</CloudDemoMode>
  <IsSamlLogin>1</IsSamlLogin>
</RemoteLaunchParemeters>
```

パラメータ:

パラメータ	説明
<ServerIP>	管理サーバのIPアドレスを指定します。
<DomainName>	Multi-Domain Security Management Serverに接続する際のDomain Management Serverオブジェクトの名前を指定します。

パラメータ	説明
<ReadOnly>	SmartConsoleを読み取り専用モードで開くかどうかを指定します。 有効な値： ■ False- SmartConsoleを書き込みモードで開きます。 ■ True- SmartConsoleを読み取り専用モードで開きます。
<CloudDemoMode>	デモモードを有効にするかどうかを指定します。 有効な値： ■ False- SmartConsoleを通常モードで開きます。 ■ True- SmartConsoleをデモモードで開きます。
<IsSamlLogin>	SAMLログインを有効にするかどうかを指定します。 有効な値： ■ 1- SAMLログインを有効にします。 ■ 0- SAMLログインを無効にします。

IPアドレス172.30.44.55のSecurity Management Serverの設定ファイルの例：

```
<?xml version="1.0" encoding="utf-8"?>
<RemoteLaunchParemeters
xmlns:xsi="http:/www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http:/www.w3.org/2001/XMLSchema">
  <ServerIP>172.30.44.55</ServerIP>
  <ReadOnly>False</ReadOnly>
  <CloudDemoMode>False</CloudDemoMode>
  <IsSamlLogin>1</IsSamlLogin>
</RemoteLaunchParemeters>
```

SAML認証を設定した後、さらに、証明書ファイルによる認証を設定できます。管理者は、SAML IDプロバイダまたは証明書ファイルを使用して、SmartConsoleを認証できます。

SmartConsoleで証明書ファイルを作成します。管理者は証明書を使用して、SmartConsoleに2つの方法でログインできます：

- SmartConsoleに**Certificate File**オプションでログインします。証明書ファイルを使用するには、管理者がパスワードを提供する必要があります。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。管理者は、この保存された証明書を使用して、CAPI証明書オプションを使用してSmartConsoleにログインできます。管理者がログインする際にパスワードを入力する必要はありません。

管理者は、他の管理者に証明書を渡して、自分の管理者アカウントなしでSmartConsoleにログインさせることもできます。

APIキー認証による管理者アカウントの作成

APIキーは、クライアントがAPIを呼び出す際に提供するトークンです。

APIキー認証は、管理者が通常の管理者名/パスワードの代わりにトークンを使用してAPIインタフェースを認証する機能を提供します。

管理者が管理用APIを使用するためのAPIキーをSmartConsoleで設定することができます。

注 - この管理者は、APIコマンドの実行にのみAPIを使用でき、SmartConsoleの認証には使用できません。

前提条件:

必要な権限プロファイルが設定されていることを確認してください。参照: *管理者への権限プロファイルの割り当て (116ページ)*。

SmartConsoleを使用して、管理者のAPI認証を設定する手順

1. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。。
2. **Permissions & Administrators**を展開 > **Administrators** をクリック。
3. 上部のツールバーから、アイコン (**New**) をクリック > **New Administrator** をクリック。

   New Administrator ウィンドウが開き、**General** ページが表示されます。
4. 一番上のフィールドに、該当するオブジェクト名を入力。
5. **オプション:** コメントを入力。
6. **Authentication Method**フィールドで、**API Key**を選択します。
7. **Generate API key**をクリック:
   a. クリック**Copy Key to Clipboard**
   b. キーは後で使用するために保存します(関連する管理者に提供するなど) 。
   c. クリック**OK**。
8. **Permission Profile**フィールドで、該当するプロファイルを選択します。
9. **Expiration**セクションで、必要な有効期限を設定します。
10. **オプション: Additional Info**ページで次を設定 :
    - **Phone Number**
    - **Contact Details**
    - **Email**

11. クリックOK。
12. SmartConsoleセッションを公開する。

例

この例では、APIコマンド"`login`"とAPIコマンド"`add simple-gateway`"に対してAPIキーを使用する方法を示します。

1. セキュリティ管理サーバのコマンド ラインに接続します。
2. エキスパート モードにログインします。
3. APIコマンド"`login`"を実行し、事前に生成したAPIキーを使用し、出力をファイルに保存します:

   構文:

   ```
   mgmt_cli login api-key <api-key> > /<path_to>/<filename>
   ```

   例:

   ```
   mgmt_cli login api-key mvYSiHVmlJM+J0tu2FqGag12 >
   /var/tmp/token.txt
   ```

4. APIコマンド"`add simple-gateway`"を実行します。

   `mgmt_cli`コマンドに"**-s**"フラグを付けて実行しトークンファイルを指定します。

   構文:

   ```
   mgmt_cli -s /<path_to>/<filename> add simple-gateway name
   <gateway name> ip-address <ip address> one-time-password
   <password> blade <true>
   ```

   例:

   ```
   mgmt_cli -s /var/tmp/token.txt add simple-gateway name
   "gw1" ip-address 192.168.3.181 one-time-password "aaaa"
   firewall true vpn true
   ```

   詳細 : *Check Point Management API Reference*。

API認証を設定した後、さらに証明書ファイルによる認証も設定できます。管理者は、API Keyまたは証明書ファイルのいずれかを使用して、Security Management Serverを認証できます。

SmartConsoleで証明書ファイルを作成します。管理者は証明書を使用して、SmartConsoleに2つの方法でログインできます:

- SmartConsoleに**Certificate File**オプションでログインします。証明書ファイルを使用するには、管理者がパスワードを提供する必要があります。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。管理者は、この保存された証明書を使用して、CAPI証明書オプションを使用してSmartConsoleにログインできます。管理者がログインする際にパスワードを入力する必要はありません。

管理者は、他の管理者に証明書を渡して、自分の管理者アカウントなしでSmartConsoleにログインさせることもできます。

管理者への権限プロファイルの割り当て

権限プロファイルとは、管理者に割り当てることのできる、Security Management ServerおよびSmartConsoleの管理者権限の定義済みセットです。権限プロファイルは、複数の管理者に割り当てることができます。権限プロファイルを作成および管理できるのは、プロファイルに*管理者を管理*権限を持つSecurity Management Server管理者のみです。

マルチドメインセキュリティ管理管理者用の権限プロファイルについての詳細：*R82 Multi-Domain Security Management Administration Guide*。

権限プロファイルの変更と作成

スーパーユーザ権限を持つ管理者は、権限プロファイルの編集、作成、削除を行うことができます。

これらは、定義済みのデフォルト権限プロファイルです。デフォルトの権限プロファイルを変更または削除することはできません。複製して、その複製したクローンを変更することができます。

- **Read Only All** - 完全な読み取り権限。書き込み権限はなし。
- **Read Write All** - 完全な読み取り/書き込み権限。
- **スーパーユーザ** - 管理者とセッションの管理を含む、完全な読み取りと書き込みの権限。

注 - 複数の管理者が同時に、**Read-Write All**権限でSmartConsoleにログインできます。**Read Only All**と**Read-Write All**の権限プロファイルを切り替えることはできません。モードを切り替えるには、セッションを終了し、SmartConsoleに再接続して、SmartConsoleのログイン画面で、必要に応じて**Read Only**のチェックボックスをオンまたはオフにします。

管理者の権限プロファイルを変更するには

1. **Manage & Settings** >**Permissions & Administrators** をクリックします。
2. 管理者アカウントをダブルクリックします。

   Administratorsプロパティウィンドウが表示されます。
3. **Permissions**セクションで、リストから別の**Permission Profile**を選択します。
4. **OK**をクリックします。

権限プロファイルを変更するには

1. SmartConsoleで、**Manage & Settings** > **Permissions & Administrators** > **Permission Profiles** と進みます。
2. 変更するプロファイルをダブルクリックします。
3. 開いた**Profile**の設定ウィンドウで、必要に応じて設定を変更します。
4. クリック**Close**。

新しい権限プロファイルを作成するには

1. SmartConsoleで、**Manage & Settings** > **Permissions & Administrators** > **Permission Profiles** と進みます。
2. **New Profile**をクリックします。

   New Profileウィンドウが開きます。
3. プロファイルの一意な名前を入力します。
4. プロファイルの種類を選択します。
   - **Read/Write All**- 管理者はすべての機能に変更を加えることができます
   - **Auditor (Read Only All)**- 管理者はすべての情報を確認できますが変更はできません
   - **Customized**- カスタム設定 (*カスタマイズされた権限の設定 (118ページ)*)。
5. クリック**OK**。

権限プロファイルを削除するには

1. SmartConsoleで、**Manage & Settings** > **Permissions & Administrators** > **Permission Profiles**と進みます。
2. プロファイルを選択して、**Delete**をクリックします。

   管理者に割り当てられたプロファイルは、削除できません。どの管理者がプロファイルを使用しているかを確認するには、エラーメッセージの中で**Where Used**をクリックします。

   管理者にプロファイルが割り当てられていない場合は、確認画面が表示されます。
3. **Yes**をクリックして確定します。

カスタマイズされた権限の設定

Gateways、Access Control、Threat Prevention、Others、Monitoring and Logging、Events and Reports、Managementの管理者権限を設定します。各リソースについて、このプロファイルで構成される管理者が機能を設定できるか、または表示されるだけかを定義します。

権限:

- **Selected**- 管理者にこの機能があります。
- **Not selected**- 管理者にこの機能はありません。

注 - 機能選択をクリアできない場合、その機能への管理者アクセスは必須です。

一部の機能には、ReadとWriteのオプションがあります。機能が選択されている場合:

- **Read**- 管理者はこの機能はあるが変更はできません。
- **Write**- 管理者はこの機能があり変更できます。

カスタマイズされたアクセス許可を設定するには

1. Profileオブジェクトの**Overview > Permissions**セクションで、**Customized**を選択します。
2. Profileオブジェクトのこれらのページで権限を設定します。
   - **GatewaysProvisioning**、**Scripts**権限を設定します。
   - **Access Control**- アクセスコントロールポリシーの権限を設定します。*アクセスコントロールと脅威対策のためのアクセス許可の設定 (121ページ)*)。
   - **Threat Prevention**- 脅威対策ポリシーのアクセス許可を設定します。*アクセスコントロールと脅威対策のためのアクセス許可の設定 (121ページ)*)。
   - **Others**-**Common Objects**、ユーザデータベース、**HTTPS Inspection**機能、**Client Certificates**に対する権限を設定します。
   - **Monitoring and Logging**- ログの生成と表示、およびモニタリング機能の使用許可を設定 (*モニタ、ログ、イベント、レポートの権限の設定 (122ページ)*)。
   - **Events and Reports**- SmartEvent機能の権限を設定 (*モニタ、ログ、イベント、レポートの権限の設定 (122ページ)*)。
3. **Management**セクションで、このプロファイルに次の権限を設定します。
   - **Manage Administrators**- その他の管理者アカウントの管理
   - **Manage Sessions**- 他の管理者セッションを切断、破棄、公開、または引き継ぐことができます。
   - **High Availability Operations**- ハイアベイラビリティの設定と作業。

- **Management API Login**- Security Management Serverにログインし、これらのツールを使用してAPIコマンドを実行する権限：
  - `mgmt_cli`(LinuxとWindowsのバイナリ)
  - Gaia CLI (clish)
  - Webサービス(REST)

  管理者が管理サーバ上で自動スクリプトを実行できないようにする場合に便利です。

  注 - SmartConsoleのAPIターミナルからコマンドを実行する場合、この権限は必要ありません。
- **Cloud Management Extension (CME) API**- クラウド管理拡張 (CME) 構成の読み取りまたは編集の許可。
- **Publish sessions without an approval**- 承認なしに出版することを許可する。
- **Approve / reject other sessions**- 他のセッションを承認または拒否する権限を持つ。
- **Manage integration with Infinity Services**- SmartConsoleの**Infinity Services**ビューからInfinity Portalへの接続許可。

4. クリック**OK**。

重要- 権限プロファイルにおいて、**VSX Provisioning** ([Gateway]タブ内) を選択した場合、**Publish sessions without an approval** ([**Management**]タブ内) も選択する必要があります。これは、管理サーバがVSXオブジェクトの変更を直ちに保存する必要があるためです。

アクセスコントロールレイヤーの権限の設定

異なるレイヤーの所有権を異なる管理者に委任することで、アクセスコントロールポリシーの管理を簡素化することができます。

これを行うには、レイヤーに権限プロファイルを割り当てます。権限プロファイルには次の権限が必要です: **Edit Layer by the selected profiles in a layer editor**。

この権限を備えた権限プロファイルを持つ管理者は、レイヤーを管理することができます。

ワークフロー

1. 管理者プロファイルにレイヤー権限を付与します。
2. レイヤーに権限プロファイルを割り当てます。

管理者プロファイルにレイヤー権限を付与するには

1. **Profile**オブジェクトの**Access Control > Policy**セクションで、**Edit Layer by the selected profiles in a layer editor**を選択します。
2. クリック**OK**。

権限プロファイルをレイヤーに割り当てるには

1. SmartConsole で、**Menu > Manage policies and layers**をクリックします。
2. 左側のペインで**Layers**をクリックします。
3. レイヤーを選択します。
4. クリック**Edit**。
5. 左側のペインで**Permissions**を選択します。
6. クリック**+**
7. レイヤー権限のあるプロファイルを選択します。
8. クリック**OK**。
9. クリック**Close**。
10. SmartConsoleセッションを公開する。

アクセスコントロールと脅威対策のためのアクセス許可の設定

権限プロファイルオブジェクトで、機能を選択し、その機能に対する読み取りまたは書き込みの管理者権限を選択します。

- Access Control

  レイヤーを編集するには、レイヤー内のすべてのSoftware Bladeの権限が必要です。

  Actionsセクションで:

  - Install Policy- セキュリティゲートウェイにアクセスコントロールポリシーをインストールします。
  - Application & URL Filtering Update- アクセスルールに使用するアプリケーションやWebサイトの新しいパッケージをダウンロードし、インストールします。

- Threat Prevention

  Actionsセクションで:

  - Install Policy- セキュリティゲートウェイに脅威対策ポリシーをインストールします。
  - IPS Update-IPS保護用の新しいパッケージをダウンロードし、インストールします。

モニタ、ログ、イベント、レポートの権限の設定

Profileオブジェクトで、機能とその管理者権限である読み取り/書き込みを選択します。

- **モニタリングとログ機能**

  これらは利用可能な機能の一*部*です:

  - Monitoring
  - Management Logs
  - Track Logs
  - Application and URL Filtering Logs

- **イベントとレポート機能**

  SmartEventに関する権限です。

  - SmartEvent
    - **Events**- SmartConsoleのビュー**Logs & Events**
    - **Policy**- SmartEvent GUIの**SmartEvent Policy and Settings**。
    - **Reports**- SmartConsole >**Logs & Events**
  - SmartEvent Application & URL Filtering reports only

信頼できるクライアントの定義

指定したホスト一覧からのSecurity Management Serverへのアクセスを制限するには、**Trusted Clients**を設定する必要があります。

Trusted Clientsは、このような方法で設定することができます。

信頼できるクライアントの定義	説明
Any	すべてのホスト
IPv4 Address	指定されたIPv4アドレスを持つ単一ホスト
IPv4 Address Range	指定した範囲内のIPv4アドレスを持つホスト
IPv4 Netmask	指定されたIPv4アドレスとネットマスクで定義されたサブネットに属するIPv4アドレスを持つホスト
IPv6 Address	指定されたIPv6アドレスを持つ単一ホスト
IPv6 Address Range	指定した範囲内のIPv6アドレスを持つホスト
IPv6 Netmask	指定されたIPv6アドレスとネットマスクで定義されたサブネット内のIPv6アドレスを持つホスト
Name	指定されたホスト名を持つホスト
Wild cards (IP only)	指定された正規表現で記述されたIPアドレスを持つホスト

スーパーユーザの権限を持つ管理者は、SmartConsoleで信頼できるクライアントを追加、編集、または削除することができます。

新しい信頼できるクライアントの追加

1. SmartConsoleで、**Manage & Settings** > **Permissions & Administrators** > **Trusted Clients**に進みます。
2. **New**をクリックします。

   New Trusted Clientウィンドウが開きます。
3. クライアントの固有名を入力します。
4. クライアントタイプを選択し、対応する値を設定します。
   - **Any**- 設定する値なし
   - **IPv4 Address**- ホストのIPv4アドレスを入力
   - **IPv4 Address Range**- IPv4アドレス範囲の最初と最後のアドレスを入力
   - **IPv4 Netmask**- IPv4アドレスとネットマスクを入力
   - **IPv6 Address**- ホストのIPv6アドレスを入力
   - **IPv6 Address Range**- IPv6アドレス範囲の最初と最後のアドレスを入力
   - **IPv6 Netmask**- IPv6アドレスとネットマスクを入力
   - **Name**- ホスト名を入力
   - **Wild cards (IP only)**- IPアドレスのセットを記述する正規表現を入力
5. クリック**OK**。

信頼できるクライアント設定の変更

1. SmartConsole で、**Manage & Settings** > **Permissions & Administrators** > **Trusted Clients**に進みます。
2. 編集するクライアントをダブルクリックします。
3. 開いた**Trusted Client**の設定画面で、必要に応じて設定を変更します。
4. クリック**OK**。

信頼できるクライアントの削除

1. SmartConsole で、**Manage & Settings** > **Permissions & Administrators** > **Trusted Clients**に進みます。
2. 信頼できるクライアントを選択し、**Delete**をクリックします。

   確認画面が表示されます。
3. **Yes**をクリックして確定します。

注 - 管理者は、セキュリティ管理サーバ上のCheck Point設定ツールで**GUI Clients**を構成することもできます(*cpconfig (743ページ)*)。

管理者向けセッションフロー

SmartConsoleでは、管理者はセッションで作業します。セッションは、管理者がSmartConsoleにログインするたびに作成されます。セッションで行った変更は、自動で保存されます。セッションで行われたすべての変更を表示する変更レポートを作成することができます。これらの変更は非公開で、管理者のみが利用できます。設定の競合を避けるため、他のセッションで編集中のオブジェクトやルールには、他の管理者にロックアイコンが表示されます。

管理者は、プライベートな変更内容を公開したり、破棄したりすることができます。プライベートの変更をポリシーのインストールに含めるには、セッションで変更を公開する必要があります。これは、プライベートな変更を他の管理者が利用できるようにしたい場合にも当てはまります。他のセッションからの未公開の変更は、ポリシーのインストールに含まれません。

セッションを公開する前に、セッションに名前を付け、作業工程を記録する簡単な説明を追加することをお勧めします。

セッションの公開

SmartConsoleの検証ペインには、設定エラーメッセージが表示されます。エラーの例としては、一意でないオブジェクト名や、ルールベースで有効でないオブジェクトの使用などがあります。公開する前に、これらのエラーを必ず修正してください。

SmartConsoleのセッションを公開するには

SmartConsoleツールバーで、Publishをクリックします。セッションが公開されると、新しいデータベースバージョンが作成され、データベースリビジョンのリストに表示されます。

セッションに名前または説明を追加するには

1. SmartConsoleツールバーで、Sessionをクリックします。

   Session Detailsウィンドウが開きます。
2. データベースのバージョン名を入力します。
3. 説明を入力します。
4. クリックOK。

セッションを破棄するには

SmartConsoleツールバーで、Discardをクリックします。

SmartConsoleのセッションビューでの作業

セッションビューには、システム内のすべての未公開セッションが表示されます。このビューには、現在の管理者のセッション、他の管理者のセッション、および他のアプリケーションのセッションが表示されます。ビューのカラムはカスタマイズ可能で、セッションの所有者、名前、説明、接続モード、プライベートの変更回数、ロック回数、アプリケーションなどの値を表示します。

セッション情報を見るには、**Manage & Settings** >**Sessions** >**View Sessions**をクリックします。

プライベートセッションで管理者が利用できるアクションは、プロファイルの**Manage Sessions**権限によって決定されます。

セッションの管理権限を持たない管理者ができること:	セッションの管理権限を持つ管理者ができること:
■ 自分のセッションを公開および破棄する ■ 他の管理者が開いているセッション、その管理者のロック数、その管理者が行った変更数などの確認 ■ アプリケーションによって作成されたセッションを引き継ぐ(例 : APIコマンドラインツールによって作成されたセッションなど)	■ 自分のセッションを公開および破棄する ■ 他の管理者が開いているセッション、その管理者のロックの数、その管理者が行った変更の数などの確認 ■ **Publish & Disconnect**他の管理者のプライベートセッション ■ **Disconnect & Discard**他の管理者のプライベートセッション ■ **Disconnect**別の管理者のプライベートセッション ■ **Take over**アプリケーションによって作成されたセッション(APIコマンドラインツールによって作成されたセッションなど ■ **Take over**他の管理者のプライベートセッション **注** - 自分のプライベートセッションで行った変更を保持したい場合は、他の管理者のセッションを引き継ぐ*前に*、これらの変更を公開してください。変更内容を公開しないと、変更内容が失われてしまいます。引き継ぐ際には、もう一人の管理者のSmartConsoleのセッションを切断します。 ■ **Publish & Disconnect**他の管理者のプライベートセッションこのアクションは、SmartConsoleセッションとコマンドラインAPIセッションの両方に適用されます。 ■ **Disconnect**他の管理者のプライベートセッション ■ **Discard & Disconnect**他の管理者のプライベートセッション

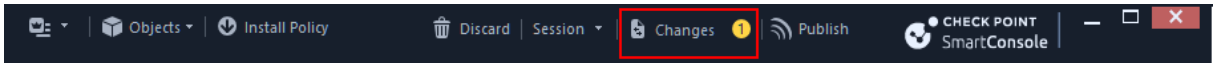
プライベートセッションで行った変更の表示

特定のセッションで行われた変更を表示するレポートを作成することができます。現在のセッションでも別のセッションでもかまいません。セッションで行われた変更を追跡することで、行われた変更を追跡モニタリングし、バグのトラブルシューティングを行うことができます。

変更レポートでは、ポリシールールと共通ネットワークオブジェクトの変更のみが記載されます。詳細：sk166435

現在のセッションで行われた変更を表示するには:

ツールバーのChanges ボタンをクリックします。



現在のプライベートセッションで行われた変更を示すレポートが作成されます。

任意のセッションで行われた変更を表示するには

1. SmartConsole で、**Manage & Settings** >**Sessions** >**View Sessions** を開きます。

   セッションのリストが表示されます。

2. 必要なセッションをクリックします。

3. ツールバーのChangesボタンをクリックします。

   変更レポートが作成されます。

   レポートには、選択したプライベートセッションの比較が表示されます。

注 - セッションツールバーとリビジョンビューに表示される変更回数には不一致があります。

非アクティブなセッションを持つ管理者からロックされたオブジェクトを引き継ぐ

SmartConsoleに、セッションが無効になっている管理者がロックしたオブジェクトがある場合、該当する管理者が現在SmartConsoleにログインし直してロックを解除することができない場合、その管理者のセッションを引き継ぐことができます。

他の管理者の非アクティブセッションを引き継ぐには

1. 別の管理者アカウントでSmartConsoleにログインします。

2. 管理と設定 >**Sessions** > **View Sessions**にアクセスします。

3. ロックされたオブジェクトを所有する管理者の該当セッションを右クリックし、**Take over**を選択します。

これで、関連するオブジェクトを開き、変更を公開または破棄してロックを解除することができます。

複数のセッションで作業する管理者

複数のセッションで作業している管理者は、現在のプライベートセッションで行われた変更を公開することなく、さらに複数のプライベートセッションを開くことができます。

使用事例

プライベートセッションで変更を加えているときに、何か差し迫った問題を解決するように求められたとします。解決には、変更を加えて公開する必要があるとします。現在のプライベートセッションは、公開や破棄したくありません。

新しいプライベートセッションを開き、問題解決に必要な変更を行い、その変更を公開してから、以前のプライベートセッションに戻ります。

そのためには、複数のセッションで作業する必要があります。複数のセッション間で切り替えを行うには、管理者プロファイルで**Manage Sessions**権限を選択する必要があります。

複数セッションの作業を有効にするには

1. 該当する権限プロファイルを開きます。
2. **Management**ページで、**Manage Sessions**権限が選択されていることを確認します。
3. **SmartConsole >Manage & Settings**ビュー **>Sessions >Advanced** を開きます。
4. **Each administrator can manage multiple SmartConsole sessions at the same time**を選択します。
5. **Publish**。

複数のセッションで作業する場合：

- 同じ管理者アカウントを使用して、Security Management Serverへの複数のセッションを開き、管理することが可能
- アクティブなセッションと過去に保存したセッションの切り替えが可能
- 他のセッションの公開、破棄、切断が可能
- 他のセッションを引き継げる

SmartConsoleセッションメニュー

複数のセッションを有効にすると、SmartConsoleのセッションメニューに以下の新しいオプションが表示されます。

オプション	説明
Edit sessions details	セッション名と説明を変更できます。

オプション	説明
Create new session	**In the current window** 現在のSmartConsoleで新しいセッションを開始します。 **In a new window** 新しいSmartConsoleで新しいセッションを開始します。
Recent	最近のセッションの一覧を表示します。セッションを選択すると、現在のSmartConsoleでセッションが開きます。
More	以前に作成・保存したセッションを表示するウィンドウ(**Open Session**) を開きます。 ■ このウィンドウに表示されるセッションは、現在のドメインの現在の管理者が所有しています。 ■ **Open Session > Actions**メニューには、保存したセッションを現在のSmartConsoleで開いたり、新しいSmartConsoleで開いたりするオプションがあります。

SmartConsoleセッションビュー

複数セッションが有効な場合、以下の追加アクションが可能です。

アクション	以下を実行できます。
所有するセッション	■ 廃棄と切断 ■ 公開と切断 ■ 切り離す ■ 古いセッションを開く
他の管理者が所有し、プライベート変更を行ったセッションの場合	■ 変更内容の公開と切断 ■ 廃棄と切断 ■ 切り離す ■ 変更を引き継ぐ
他の管理者が所有し、プライベートセッションを作成していないセッションの場合	■ 切り離す ■ 引き継ぐ

注

- シングルセッションで作業する場合、別のセッションを引き継ぐ前に、変更内容を公開するか破棄する必要があります。複数セッションの場合、他の管理者のセッションを引き継ぐ前に、自分のセッションを公開したり破棄したりする必要はありません。
- 複数セッションの場合、すでに接続しているセッションに別のデスクトップから接続した管理者は、デフォルトで接続しているセッションを引き継ぐことができます。

マルチセッションとシングルセッションの切り替え

セッション管理の設定が、複数のSmartConsoleセッションから、一度に1つのSmartConsoleセッションしか許可しないように切り替わった場合：

- 管理者は、引き続き自分が所有するセッションを公開、廃棄、開くことができます。
- プライベートセッションで未公開のセッションをすべて公開するか破棄するまで、新しいセッションを作成することはできません。
- 他の管理者やアプリケーションのセッション(*mgmt_cli*ユーティリティのAPIコマンドで作成されたセッションなど) は、以前に保存したプライベートセッションをすべて公開するか破棄するまで引き継ぐことができません。

セッションの承認サイクル(SmartWorkflow および Identity Provider)

管理者は、他の管理者が行ったセッションの変更を承認できます。

使用事例

この機能により、他の管理者が行った設定変更を公開する前に確認し、承認することができます。どの管理者が変更を承認のために提出しなければならないか、どの管理者に変更を承認する権限があるかを定義できます。

設定

1. **変更が承認を必要とする管理者 "A"の新しい権限プロファイルを作成します。**

    a. SmartConsoleで、**Manage & Settings** >**Permissions & Administrators** > **Permission Profiles** > **New Profile**へ移動します。

    New Profileウィンドウが開きます。

    b. 概要ページで、**Read/Write All**または**Customized**を選択します。

    c. **Management** ページで、**Publish sessions without an approval** オプションをクリアします。

    d. 残りのプロファイル設定を構成し、**OK**をクリックして変更を公開します。

2. **変更が承認を必要とする管理者 "A"の新しい管理者アカウントを作成します:**

    a. SmartConsoleで、**Manage & Settings** > **Permissions & Administrators** > **Administrators** > **New Administrator** へ移動します。

    New Profileウィンドウが開きます。

    b. 管理者名とその他のプロパティを設定し、**Permission Profile**フィールドで、この管理者用に作成したプロファイルを選択します。

    c. **OK**をクリックします。

3. **変更を承認する管理者 "B"の新しい権限プロファイルを作成します。**

    a. SmartConsoleで、**Manage & Settings** >**Permissions & Administrators** >**Permission Profiles** >**New Profile** へ移動します。

    New Profileウィンドウが開きます。

    b. 概要ページで、**Read/Write All**または**Customized**を選択します。

    c. **Management**ページで**Approve/reject other sessions**を選択します。

    d. 残りのプロファイル設定を行い、**OK**をクリックします。

4. **変更を承認する管理者 "B"の新しい管理者アカウントを作成します:**

   a. SmartConsoleで、**Manage & Settings** >**Permissions & Administrators** >**Administrators** >**New Administrator** へ移動します。

      New Profileウィンドウが開きます。

   b. 管理者名とその他のプロパティを設定し、**Permission Profile**フィールドで、この管理者用に作成したプロファイルを選択します。

   c. **OK**をクリックし、変更を公開します。

5. **変更の承認を得るには、SmartConsoleの上部ツールバーで「リクエストの送信」をクリックします。**

   注 - 管理者「A」が、自分の変更が承認される前にポリシーをインストールしようとすると、最初に変更を承認に提出する必要があることを示すメッセージが表示されます。

   管理者 "A"がSmartConsoleの設定変更をするたび:

   管理者 "A"がルールベースのルールを変更して**Submit**をクリックすると、SmartConsoleはこのルールをロックし、以降の変更を禁止し、鍵のアイコンが表示されます。

   管理者 "A"がオブジェクトを変更して**Submit**をクリックすると、SmartConsoleでこのオブジェクトがロックされます。オブジェクトのプロパティを表示することしかできません(オブジェクトを右クリック > **View**) 。

   注 - 全セッションのステータスを確認するには、管理 & 設定 > **Sessions** >**View Sessions** を開きます。

6. **管理者 "B "が変更を確認、承認します。**

   注 - 承認待ちのセッションがある場合、**Manage & Settings**タブと**View Sessions**タブの横に、承認待ちのセッション数を示す通知が表示されます。

   a. SmartConsole で、**Manage & Settings** >**Sessions** >**View Sessions** に進みます。

   b. 承認待ちのセッションを右クリックします。

   c. 変更を確認するには、ドロップダウンメニューから**Review change report**を選択します。

d. 変更内容を確認したら、セッションを右クリックし、ドロップダウンメニューから以下のいずれかのオプションを選択します:

- セッションを公開するには、**Approve** を選択します。セッションが公開された後、管理者"A"はポリシーをインストールできます。
- セッションを修正するために提出者に戻すには、**Reject**を選択します。このオプションを選択すると、セッションは管理者「A」に戻ります。ウィンドウが開き、理由を記入する必要があります。

7. **管理者"A"は、管理と設定タブとセッションの表示タブで、レビューされたセッションの通知を確認できます。**

セッションを修正するには、セッションをクリックし、ドロップダウンメニューから**open session**を選択します。

注

- セッションの更新に関するEメール通知を受け取るには、**Manage & Settings** > SmartTasksに移動し、該当するSmartTaskを設定します(*SmartTasks (600ページ)*)。
- データベースツールまたはSmartProvisioningで変更を保存するには、承認なしで変更を公開する権限が必要です。**Publish sessions without an approval**オプションがクリアされている場合、データベースツールやSmartProvisioningで変更を保存することはできません。

チームワークのセッティング

管理者として、オブジェクトやユーザの定義などのタスクを他の管理者に委任することができます。必ず、タスクを完了するために必要な権限を持つ管理者アカウント (*管理者アカウントの管理 (74 ページ)*)を作成してください。

自身が唯一の管理者である場合、トラブルシューティング、コンサルテーション、または監査に便利な、読み取り専用権限を持つ2番目の管理者アカウントを作成することをお勧めします。

ユーザアカウントの管理

ユーザアカウントは、Check Point環境でトラフィックを生成するユーザを表すオブジェクトです。管理サーバの管理者は、ユーザアカウントを作成、管理、およびモニタします。セキュリティゲートウェイでは、認証されたユーザのアクセス権限を制御することができます。管理者は、セキュリティルールベースを使用して、指定されたリソースへのアクセスをユーザに制限または許可します。ユーザは自分が属しているグループは知りません。機密情報やリソースへのアクセスを許可されたユーザのみに制限することで、組織のネットワークとデータのセキュリティを確保します。

ユーザはセキュリティゲートウェイに認証されます。Check Pointは、ユーザに対してさまざまな認証方法をサポートしています。

すべてのユーザは、SmartConsoleで直接設定され(Active Directoryなどの外部サーバで設定されるユーザとは対照的) 、管理サーバ上の管理データベースに保存されます。

管理者がポリシーをインストールすると、管理サーバは該当するユーザデータを管理対象のセキュリティゲートウェイにコピーします。

管理者がデータベースをインストールすると(**Menu** >**Install Database**) 、管理サーバは該当するユーザデータを管理対象サーバ(例 : ログサーバ) にコピーします。

ユーザアカウントの作成

SmartConsole でユーザアカウントを作成する際、これらの認証方法のいずれかを選択できます:

認証方法	説明
Check Point Password	Check Pointのパスワードは、SmartConsoleに設定されている静的なパスワードです。セキュリティゲートウェイのローカルデータベースがパスワードを保存します。追加のソフトウェアは必要ありません。 参照: *Check Pointのパスワード認証を使用したユーザアカウントの作成 (146ページ)*。
OS Password	OSパスワードは、セキュリティゲートウェイがインストールされているコンピュータのオペレーティングシステムに保存されます。また、Windowsドメインに保存されているパスワードも使用することができます。追加のソフトウェアは必要ありません。 参照: *OSパスワード認証によるユーザアカウントの作成 (150ページ)*

認証方法	説明
RADIUS	RADIUS(Remote Authentication Dial-In User Service) は、外部認証方式の1つで、認証機能をアクセスサーバから分離することにより、セキュリティとスケーラビリティを実現するものです。 RADIUSを使用すると、管理者によるRADIUSグループへのユーザの割り当てに基づいて、認証されたRADIUSユーザのアクセス権限を制御できます。これらのグループは、セキュリティルールベースで、ユーザが特定のリソースにアクセスすることを制限したり、許可したりするために使用されます。ユーザは自分が属しているグループは知りません。 セキュリティゲートウェイは、リモートユーザによる認証要求をRADIUS サーバに転送します。ユーザのアカウント情報を保存しているRADIUSサーバが認証を行います。 RADIUSプロトコルはUDPを使ってセキュリティゲートウェイと通信します。 RADIUSグループを使用するには、RADIUSサーバのRADIUSユーザプロファイルにreturn属性を定義する必要があります。この属性はセキュリティゲートウェイに返され、ユーザが属するグループ名 (例えば、**RAD_<RADIUSユーザが属するグループ>**) を含みます。 Gaiaオペレーティングシステムでは、"Vendor-Specific" (26) 属性を使用します。 参照: *RADIUSサーバ認証によるユーザアカウントの作成 (154ページ)*。
TACACS	TACACS(Terminal Access Controller Access Control System) は、1つまたは複数の集中型サーバを通じて、ルータやネットワークアクセスサーバなどのネットワーク接続デバイスのアクセス制御を行うシステムです。 TACACSは、検証サービスを提供する外部認証メソッドです。TACACSでは、リモートユーザからの認証要求をTACACSサーバに転送します。ユーザのアカウント情報を保存するTACACSサーバで、ユーザ認証が行われます。物理的なカードキーデバイスやトークンカード、Kerberosの秘密キー認証に対応しています。TACACSは、すべての認証要求のユーザ名、パスワード、認証サービス、およびアカウンティング情報を暗号化し、通信の安全性を確保します。 参照: *TACACSサーバ認証によるユーザアカウントの作成 (161ページ)*

認証方法	説明
SecurID	SecurIDは、ユーザがトークン認証デバイスを所有し、PINまたはパスワードを提供することを要求します。トークン認証は、RSA認証マネージャ(AM) に同期するワンタイムパスワードを生成するもので、ハードウェアまたはソフトウェアの形態で提供されます。ハードウェアトークンは、キーホルダーやクレジットカード大のデバイスです。ソフトウェアトークンは、ユーザが認証を希望するPCやデバイスに置かれます。すべてのトークンは、約1分ごとに変化するランダムな1回限りのアクセスコードを生成します。ユーザが保護されたリソースに対して認証を試みる場合、AMによってワンタイムのコードが検証される必要があります。 セキュリティゲートウェイは、リモートユーザによる認証要求をAM に転送します。AMは、RSAユーザのデータベースと、割り当てられたハードトークンまたはソフトトークンを管理します。セキュリティゲートウェイはAMエージェントとして機能し、すべてのアクセス要求をAMに送り認証します。エージェント構成の詳細については、RSA Authentication Managerのドキュメントを参照してください。SecurID認証方式に必要なパラメータは特にありません。認証リクエストは、SDKがサポートするAPIまたはREST APIを介して送信できます。 参照: *SecurID認証によるユーザアカウントの作成 (168ページ)*

重要 - 認証方式を選択しない場合は、ユーザはログインもしくはネットワークリソースを利用できません。

Check Pointの認証方法のいずれかを使用して認証を構成した後は、さらに、ユーザの証明書ファイルを作成することができます。ユーザは、Check Pointの認証方法のいずれか、または証明書ファイルを使用してセキュリティゲートウェイを認証できます。

SmartConsoleで証明書ファイルを作成し、ユーザはその証明書ファイルを使って2つの方法でセキュリティゲートウェイにログインできます:

- **Certificate File**オプションで セキュリティゲートウェイ にログインします。ユーザは、証明書ファイルを使用するためにパスワードが必要です。
- Microsoft Windows SmartConsoleコンピュータのWindows証明書ストアに証明書ファイルをインポートできます。ユーザは、この保存された証明書を使用して、CAPI 証明書オプションでセキュリティゲートウェイにログインできます。ユーザはログインするためのパスワードを入力する必要はありません。

既存ユーザの変更

手順

1. オブジェクトエクスプローラーで、**User/Identity** > **Users**をクリックします。
2. ユーザをダブルクリックします。

   Userウィンドウが開きます。
3. 必要に応じて、プロパティを変更してください。
4. クリック**OK**。

ユーザの削除

手順

1. オブジェクトエクスプローラーで、**User/Identity** > **Users**をクリックします。
2. アカウントを右クリックし、**Delete**を選択します。

   確認画面が表示されます。
3. **Yes**をクリックします。

ユーザグループの管理

ユーザグループは、ユーザアカウントの集合です。ルールのSourceまたはDestinationにユーザグループを追加します。個別のユーザをルールに追加することはできません。

また、ユーザグループの編集や、ルールベースで使用しないユーザグループの削除も可能です。

新しいユーザグループを作成するには

1. オブジェクトエクスプローラ(F11)で、New > More > User/Identity > User Groupをクリックします。

   New User Groupウィンドウが開きます。
2. 新しいグループの名前を入力します。
3. 各ユーザまたはユーザグループに対して、[+]記号をクリックし、リストからオブジェクトを選択します。
4. オプションの設定を行います。
   - Mailing List Address
   - Comment
   - Tag
   - Color
5. クリックOK。

新規ユーザや他のユーザグループをグループに追加するには

1. オブジェクトエクスプローラー(F11)で、Object Categories >Users/Identities > を選択します。User Groups
2. ユーザグループを右クリックし、Editをクリックします。

   User Groupウィンドウが開きます。
3. クリック+
4. ユーザまたはユーザ・グループを選択します。
5. クリックOK。

ユーザのデフォルト有効期限設定の設定

ユーザアカウントの有効期限が近づくと、SmartConsoleでユーザのプロパティを開いたときに通知が表示されます。

手順

1. メインページ**Menu**から**Global Properties**を選択します。

   Global Propertiesウィンドウが開きます。

2. **User Accounts**をクリックします。

3. **Expire at**または**Expire after**を選択します。

   - **Expire at**- カレンダーコントロールから有効期限を選択します。
   - **Expire after**- ユーザアカウントが失効するまでの日数(アカウントが作成された日から)を入力します。

4. **Show accounts expiration indication**を選択し、日数を入力します。

   SmartConsoleのユーザオブジェクトに表示される期限切れ警告には、アカウントが期限切れになるまでの日数が表示されます。この間、ユーザアカウントをより長く有効にしておきたい場合は、ユーザアカウントの有効期限設定を編集できます。これにより、労働時間の損失を防ぐことができます。

ユーザの管 理

すべてのユーザは、SmartConsoleで直 接 設 定 され(Active Directoryなどの外 部 サーバで設 定 されるユーザとは対 照 的) 、管 理 サーバ上 の管 理 データベースに保 存 されます。

管 理 者 がポリシーをインストールすると、管 理 サーバは該 当 するユーザデータを管 理 対 象 のセキュリティゲート ウェイにコピーします。

管 理 者 がデータベースをインストールすると(**Menu** >**Install Database**) 、管 理 サーバは該 当 するユーザデータを管 理 対 象 サーバ(例 : ログサーバ) にコピーします。

新しいユーザテンプレートの作 成

ユーザテンプレート はプロファイルを設 定 します - このユーザテンプレートを選 択 したすべての新 規 ユーザは、自 動 的 にこれらの設 定 を取 得 します。これらのテンプレート 設 定 は、各 ユーザオブジェクトでオーバーライド できます。

1. 右 上 にある、**Objects** パネルをクリックします。
2. **New** >**More** >**User/Identity** >**User Template** をクリックします。

   New User Templateウィンドウが開きます。
3. 一 番 上 のフィールド に、該 当 するオブジェクト 名 を入 力 します。
4. **オプション:** コメントを入 力 します。
5. **General**ページで、このオブジェクト の有 効 期 限 を設 定 します:
   - **According to Global Properties**
   - **Expire at**

     これは、ユーザがネット ワークリソースやアプリケーションへのアクセスを許 可 されなくなる日 付 です。
6. **Groups**ページで、該 当 するユーザグループオブジェクト を選 択 します。

   このユーザテンプレートを選 択 したすべての新 規 ユーザは、自 動 的 にこれらのユーザグループに追 加 されます。
7. **Authentication**ページで、認 証 方 法 を選 択 します:
   - **Undefined**
   - **Check Point Password**
   - **OS Password**
   - **SecurID**

- RADIUS
- TACACS

8. **Location** のページで次を行います。
   a. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可されたソースを設定します。

      これらのオブジェクトは、選択する前にすでに存在している必要があります。

   b. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可された宛先を設定します。

      これらのオブジェクトは、選択する前にすでに存在している必要があります。

9. **Time**ページで、ユーザがアクセス認証される営業日または営業時間を設定するアプリケーションです。
10. **Encryption**ページで、リモートアクセスVPNのIKEv2認証と暗号化の設定を行います。
    a. **IKE**を選択します。
    b. クリック**Edit**。

       暗号化**IKE Phase 2 Properties**ウィンドウが開きます。

    c. **Authentication**ページで、認証スキームを選択します:
       i. **Password**- ユーザは事前に共有された秘密のパスワードで認証します。
       ii. **Public Key**- ユーザは、証明書ファイルに含まれる公開鍵で認証を行います。
    d. クリック**OK**。
11. クリック**OK**。
12. SmartConsoleセッションを公開する。

新規ユーザの作成

次を参照してください。

- *Check Pointのパスワード認証を使用したユーザアカウントの作成 (146ページ)*
- *OSパスワード認証によるユーザアカウントの作成 (150ページ)*
- *RADIUSサーバ認証によるユーザアカウントの作成 (154ページ)*
- *TACACSサーバ認証によるユーザアカウントの作成 (161ページ)*
- *SecurID認証によるユーザアカウントの作成 (168ページ)*

既 存 ユーザの編 集

1. 右 上 にある、**Objects**パネルをクリックします。
2. **Object Categories**のリスト で、**Users/Identities**をクリックします。
3. **Users**をクリックします。
4. 該 当 するユーザオブジェクト をダブルクリックします。

   Userウィンド ウが開きます。
5. 必 要 な設 定 を行 います。
6. クリック**OK**。
7. SmartConsoleセッションを公 開 する。
8. アクセスコント ロールポリシーをインスト ールします。

ユーザの削 除

1. 右 上 にある、**Objects**パネルをクリックします。
2. **Object Categories**のリスト で、**Users/Identities**をクリックします。
3. **Users**をクリックします。
4. ユーザオブジェクト を右 クリックし、**Delete**を選 択 します。
5. **Yes**をクリックして確 定 します。
6. SmartConsoleセッションを公 開 する。
7. アクセスコント ロールポリシーをインスト ールします。

ユーザのデフォルト有 効 期 限 設 定 の設 定

ユーザアカウント の有 効 期 限 が近 づくと、SmartConsoleでユーザのプロパティを開 いたときに通 知 が表 示 されます。

デフォルト の有 効 期 限 を設 定 するには

1. Menuから、Global Propertiesを選 択 します。

   Global Propertiesウィンドウが開 きます。

2. User Accountsをクリックします。

3. Expire atまたはExpire afterを選 択 します。

   - Expire at- カレンダーコントロールから有 効 期 限 を選 択 します。
   - Expire after- ユーザアカウント が失 効 するまでの日 数 (アカウント が作 成 された日 から) を入 力 します。

4. Show accounts expiration indicationを選 択 し、日 数 を入 力 します。

   SmartConsoleのユーザオブジェクト に表 示 される有 効 期 限 の警 告 には、アカウント が期 限 切 れになるまでの日 数 が表 示 されます。この間 、ユーザアカウント をより長 く有 効 にしておきたい場 合 は、ユーザアカウント の有 効 期 限 設 定 を編 集 できます。これにより、作 業 時 間 のロスを防 ぐことができます。

5. クリックOK。

6. SmartConsoleセッションを公 開 する。

Check Pointのパスワード認証を使用したユーザアカウントの作成

Check Pointのパスワードは、SmartConsoleに設定されている静的なパスワードです。セキュリティゲートウェイのローカルデータベースがパスワードを保存します。追加のソフトウェアは必要ありません。

Check Pointのパスワードによる認証を設定した後は、証明書ファイルによる認証も設定できます。その後、ユーザはCheck Pointのパスワードまたは証明書ファイルを使用してセキュリティゲートウェイを認証できます。

Check Pointのパスワード認証で新規ユーザを作成するには

1. 右上にある、**Objects**パネルをクリックします。
2. **New** > **More** > **User/Identity** > **User** をクリックします。

   New Userウィンドウが開きます。
3. 該当するユーザテンプレートを選択し、**OK**をクリックします。
4. 一番上のフィールドに、該当するオブジェクト名を入力します。

   大文字と小文字を区別するユニークな文字列にしてください。

   Check Point以外の認証局でユーザ証明書を生成する場合、識別名(DN)の構成要素である共通名(CN)を入力します。

   例:

   DN: `CN = James, O = My Organization, C = My Country`

   この場合、`James`をユーザ名として入力します。

   ユーザ名としてコンテナを使用する場合、コンテナにはスペースを含まず、正確に1つの文字列を含める必要があります。
5. **オプション:** コメントを入力します。
6. **General**ページで、該当する設定を行います:
   - **Email address**(任意)
   - **Mobile phone number**(任意)

- **Expire at**

  これは、ユーザがネットワークリソースやアプリケーションへのアクセスを許可されなくなる日付です。

  デフォルトの有効期限は**Menu > Global Properties > User Accounts > Expiration Date**で設定されています。

7. **Groups**ページでは、該当するユーザグループオブジェクトを選択することができます(ユーザテンプレートで設定されたものに加えて、またはその代わりに) 。
8. **Authentication** のページで次を行います。
   a. **Authentication method**フィールドで、**Check Point Password**を選択します。

      重要 - 認証方式を選択しない場合は、ユーザはログインもしくはネットワークリソースを利用できません。

   b. **Set new password**をクリックします。
9. **Location** のページで次を行います。
   a. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可されたソースを設定します。

      これらのオブジェクトは、選択する前にすでに存在している必要があります。

   b. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可された宛先を設定します。

      これらのオブジェクトは、選択する前にすでに存在している必要があります。
10. **Time** のページで次を行います。

    ユーザに特定の勤務日または業務時間がある場合は、そのユーザがいつアクセス認証されるかを設定できます。

    - **From**および**To** - 予定勤務日の開始時刻と終了時刻を入力します。指定された範囲外の時間にログインが試みられた場合、ユーザは認証されません。
    - **Days in week**または**Daily** - ユーザがリソースを認証してアクセスできる日を選択します。このユーザは、未選択の日にログインを試みた場合、認証されません。
11. **Certificates** のページで次を行います。

    このユーザに適用される証明書を設定して、より安全なアクセスコントロールを行うことができます。

a. **New**をクリックします。

b. 該当するオプションを選択します。

- **Registration Key for certificate enrollment**

  証明書をアクティブにする登録キーを送信します。

  i. 登録キーの有効期限が切れる前に、ユーザが証明書をアクティベートできる日数を入力します。

  ii. **オプション:** コメントを入力します。

  iii. **オプション:** メールテンプレートをプレビューするには、**Template**をクリックします。

  iv. **Send**をクリックします。

  v. クリック**OK**このキーを保存します。

- **Certificate file (p12)**

  ユーザのプライベートパスワード付きの`*.p12`証明書ファイルを作成します。

  i. 証明書のパスワードを入力し、確認します。

  パスワードは、証明書ファイル内の機密データを保護するために必要です。

  ii. **オプション:** コメントを入力します。

  iii. クリック**OK**。

  iv. **Save As**ウィンドウが開くのを待ちます。

  v. **File name**フィールドでユーザ名を必ず入れます。

  vi. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

  証明書ファイルはPKCS #12形式で、拡張子は`.p12`です。

  vii. SmartConsoleコンピュータの安全な場所にアクセスします。

  viii. クリック**Save**。

  ix. ユーザにこのファイルとパスワードを渡します。

c. クリック**OK**。

注:

- ユーザがしばらくシステムにアクセスしない場合(長期休暇に入るなど)、証明書を失効させることができます。これにより、ユーザアカウントは残りますが、証明書を更新するまでアクセスすることができなくなります。
- 鍵/証明書を失効させるには、鍵/証明書を選択し、**Revoke**をクリックします。

12. **Encryption** のページで次を行います。

    リモートアクセスVPNのIKEv2認証と暗号化の設定を行うことができます。

    a. **IKE**を選択します。

    b. クリック**Edit**。

       暗号化**IKE Phase 2 Properties**ウィンドウが開きます。

    c. **Authentication**ページで、認証スキームを選択します:

       i. **Password**- ユーザは事前に共有された秘密のパスワードで認証します。

       ii. **Public Key**- ユーザは、証明書ファイルに含まれる公開鍵で認証を行います。

    d. **Encryption**ページで設定する項目はありません。

       これらのアルゴリズムは、SmartConsole > グローバルプロパティ > **Remote Access** > **VPN - Authentication** > **Encryption algorithms**セクションで設定します。

    e. クリック**OK**。

13. クリック**OK**。

14. SmartConsoleセッションを公開する。

15. アクセスコントロールポリシーをインストールします。

OSパスワード認証によるユーザアカウントの作成

OSパスワードは、セキュリティゲートウェイがインストールされているコンピュータのオペレーティングシステムに保存されます。また、Windowsドメインに保存されているパスワードも使用することができます。追加のソフトウェアは必要ありません。

オペレーティングシステムのパスワードによる認証を設定した後、証明書ファイルによる認証も設定できます。その後、ユーザはオペレーティングシステムのパスワードまたは証明書ファイルを使ってセキュリティゲートウェイを認証できます。

OSパスワード認証で新規ユーザを作成するには

1. 右上にある、**Objects**パネルをクリックします。
2. **New** > **More** > **User/Identity** > **User**をクリックします。

   New Userウィンドウが開きます。
3. 該当するユーザテンプレートを選択し、**OK**をクリックします。
4. 一番上のフィールドに、該当するオブジェクト名を入力します。

   大文字と小文字を区別するユニークな文字列にしてください。

   Check Point以外の認証局でユーザ証明書を生成する場合、識別名(DN)の構成要素である共通名(CN)を入力します。

   例:

   DN: `CN = James, O = My Organization, C = My Country`

   の場合、`James`をユーザ名として入力します。

   ユーザ名としてコンテナを使用する場合、コンテナにはスペースを含まず、正確に1つの文字列を含める必要があります。
5. **オプション:** コメントを入力します。
6. **General**ページで、該当する設定を行います:
   - **Email address**(任意)
   - **Mobile phone number**(任意)

- **Expire at**

  これは、ユーザがネットワークリソースやアプリケーションへのアクセスを許可されなくなる日付です。

  デフォルトの有効期限は**Menu** >**Global Properties** >**User Accounts** >**Expiration Date** で設定されています。

7. **Groups**ページでは、該当するユーザグループオブジェクトを選択することができます(ユーザテンプレートで設定されたものに加えて、またはその代わりに) 。
8. **Authentication** のページで次を行います。
   a. **Authentication method**フィールドで、**OS Password**を選択します。

      重要 - 認証方式を選択しない場合は、ユーザはログインもしくはネットワークリソースを利用できません。

   b. **Set new password**をクリックします。
9. **Location** のページで次を行います。
   a. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可されたソースを設定します。

      これらのオブジェクトは、選択する前にすでに存在している必要があります。

   b. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可された宛先を設定します。

      これらのオブジェクトは、選択する前にすでに存在している必要があります。
10. **Time** のページで次を行います。

    ユーザに特定の勤務日または業務時間がある場合、そのユーザがいつアクセス認証されるかを設定できます。

    - **From**および**To** - 予定勤務日の開始時刻と終了時刻を入力します。このユーザは、指定された範囲外の時刻にログインを試みた場合、認証されません。
    - **Days in week**または**Daily** - ユーザがリソースを認証してアクセスできる日を選択します。このユーザは、未選択の日にログインを試みた場合、認証されません。
11. **Certificates** のページで次を行います。

    このユーザに適用される証明書を設定して、より安全なアクセスコントロールを行うことができます。

a. **New**をクリックします。

b. 該当するオプションを選択します。

- **Registration Key for certificate enrollment**

  証明書をアクティブにする登録キーを送信します。

  i. 登録キーの有効期限が切れる前に、ユーザが証明書をアクティベートできる日数を入力します。

  ii. **オプション:** コメントを入力します。

  iii. **オプション:** メールテンプレートをプレビューするには、**Template**をクリックします。

  iv. **Send**をクリックします。

  v. クリック**OK**でこのキーを保存します。

- **Certificate file (p12)**

  ユーザのプライベートパスワード付きの`*.p12`証明書ファイルを作成します。

  i. 証明書のパスワードを入力し、確認します。

  パスワードは、証明書ファイル内の機密データを保護するために必要です。

  ii. **オプション:** コメントを入力します。

  iii. クリック**OK**。

  iv. **Save As**ウィンドウが開くのを待ちます。

  v. **File name**フィールドで、ユーザ名を必ず入れます。

  vi. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

  証明書ファイルはPKCS #12形式で、拡張子は`.p12`です。

  vii. SmartConsoleコンピュータの安全な場所にアクセスします。

  viii. クリック**Save**。

  ix. このファイルとパスワードをユーザに渡します。

c. クリック**OK**。

注:

- ユーザがしばらくシステムにアクセスしない場合(長期休暇に入るなど)、証明書を失効させることができます。これにより、ユーザアカウントは残りますが、証明書を更新するまでアクセスすることができなくなります。
- 鍵/証明書を失効させるには、鍵/証明書を選択し、**Revoke**をクリックします。

12. **Encryption** のページで次を行います。

    リモートアクセスVPNのIKEv2認証と暗号化の設定を行うことができます。

    a. **IKE**を選択します。

    b. クリック**Edit**。

       暗号化**IKE Phase 2 Properties**ウィンドウが開きます。

    c. **Authentication**ページで、認証スキームを選択します:

       i. **Password**- ユーザは事前に共有された秘密のパスワードで認証します。

       ii. **Public Key**- ユーザは、証明書ファイルに含まれる公開鍵で認証を行います。

    d. **Encryption**ページで設定する項目はありません。

       これらのアルゴリズムは、SmartConsole > Global プロパティ > **Remote Access** > **VPN - Authentication** > **Encryption algorithms**セクションで設定します。

    e. クリック**OK**。

13. クリック**OK**。

14. SmartConsoleセッションを公開する。

15. アクセスコントロールポリシーをインストールします。

RADIUSサーバ認証によるユーザアカウントの作成

RADIUS(Remote Authentication Dial-In User Service) は、外部認証方式の1つで、認証機能をアクセスサーバから分離することにより、セキュリティとスケーラビリティを実現するものです。

RADIUSを使用すると、管理者によるRADIUSグループへのユーザの割り当てに基づいて、認証されたRADIUSユーザのアクセス権限を制御できます。これらのグループは、セキュリティルールベースで、ユーザが特定のリソースにアクセスすることを制限したり、許可したりするために使用されます。ユーザは自分が属しているグループは知りません。

セキュリティゲートウェイは、リモートユーザによる認証要求をRADIUS サーバに転送します。ユーザのアカウント情報を保存しているRADIUSサーバが認証を行います。

RADIUSプロトコルはUDPを使ってセキュリティゲートウェイと通信します。

RADIUSグループを使用するには、RADIUSサーバのRADIUSユーザプロファイルにreturn属性を定義する必要があります。この属性はセキュリティゲートウェイに返され、ユーザが属するグループ名 (例えば、**RAD_<RADIUSユーザが属するグループ>**) を含みます。

Gaiaオペレーティングシステムでは、"Vendor-Specific" (26) 属性を使用します。

RADIUSサーバの設定方法については、ベンダーのドキュメントを参照してください。

ユーザは、RADIUS サーバまたはRADIUS サーバグループを通じてRADIUS 認証を実行できます。RADIUSサーバグループは、同一のRADIUSサーバからなるハイアベイラビリティなグループであり、システム内の任意またはすべてのRADIUSサーバが含まれます。グループを作成する際に、グループ内の各サーバに優先順位を定義します。優先順位の高いサーバに障害が発生すると、グループ内で次に優先順位の高いサーバに引き継がれ、その後も同様になります。すべてのRADIUSサーバに同じ優先順位を割り当てると、セキュリティゲートウェイはそのうちの 1 つをランダムに選択して認証を行います。

RADIUSサーバによる認証を構成した後、証明書ファイルによる認証も構成できます。その後、ユーザはRADIUS サーバまたは証明書ファイルを使ってセキュリティゲートウェイを認証できます。

ユーザに対するRADIUS認証の設定

1. **SmartConsoleで、新しいRADIUSサーバオブジェクトを設定します。**

    a. 右上にある、**Objects**パネルをクリックします。

    b. **New >More >Server >RADIUS** をクリックします。

    c. 一番上のフィールドに、該当するオブジェクト名を入力します。

    d. **オプション:** コメントを入力します。

    e. **Host**フィールドで、ドロップダウン矢印をクリックし、**New**をクリックします。

    f. **New Host**RADIUSサーバの**IP address**を作成します。クリック**OK**。

g. このホストがNew RADIUSウィンドウのHostフィールドに表示されていることを確認します。

h. Serviceフィールドでは、デフォルト値RADIUSのままにしておきます。

i. Shared Secretフィールドに、以前にRADIUSサーバで定義した秘密鍵を入力します。

j. Versionフィールドでは、デフォルト値RADIUS Ver. 1.0のままにしておきます。

k. Protocolフィールドでは、デフォルト値PAPのままにしておきます。

l. Priorityフィールドでは、デフォルト値1のままにしておきます。

m. クリックOK。

n. SmartConsoleセッションを公開する。

2. **新規ユーザを作成し、認証方法としてRADIUSを選択します。**

a. 右上にあるObjectsパネルをクリックします。

b. New >More >User/Identity >User をクリックします。

New Userウィンドウが開きます。

c. 該当するユーザテンプレートを選択し、OKをクリックします。

d. 一番上のフィールドに、該当するオブジェクト名を入力します。

大文字と小文字を区別するユニークな文字列にしてください。

Check Point以外の認証局でユーザ証明書を生成する場合、識別名(DN)の構成要素である共通名(CN)を入力します。

例:

DN:`CN = James, O = My Organization, C = My Country`

の場合、`James`をユーザ名として入力します。

ユーザ名としてコンテナを使用する場合、コンテナにはスペースを含まず、正確に1つの文字列を含める必要があります。

e. **オプション:** コメントを入力します。

f. **General**ページで、該当する設定を行います:

- **Email address**(任意)
- **Mobile phone number**(任意)
- **Expire at**

  これは、ユーザがネットワークリソースやアプリケーションへのアクセスを許可されなくなる日付です。

  デフォルトの有効期限は**Menu** >**Global Properties** >**User Accounts** >**Expiration Date** で設定されています。

g. **Groups**ページでは、該当するユーザグループオブジェクトを選択することができます(ユーザテンプレートで設定されたものに加えて、またはその代わりに)。

h. **Authentication** のページで次を行います。

i. **Authentication method**フィールドで、**RADIUS**を選択します。

ii. **RADIUS server**フィールドでは、デフォルト値**Any**のままにするか、該当するRADIUS サーバオブジェクトを選択します。

重要 - 認証方式を選択しない場合は、ユーザはログインもしくはネットワークリソースを利用できません。

i. **Location** のページで次を行います。

i. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可されたソースを設定します。

これらのオブジェクトは、選択する前にすでに存在している必要があります。

ii. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可された宛先を設定します。

これらのオブジェクトは、選択する前にすでに存在している必要があります。

j. **Time** のページで次を行います。

ユーザに特定の勤務日または業務時間がある場合は、そのユーザがいつアクセス認証されるかを設定できます。

- **From**および**To** - 予定勤務日の開始時刻と終了時刻を入力します。このユーザは、指定された範囲外の時刻にログインを試みた場合、認証されません。
- **Days in week**または**Daily** - ユーザがリソースを認証してアクセスできる日を選択します。このユーザは、未選択の日にログインを試みた場合、認証されません。

k. **Certificates** のページで次を行います。

このユーザに適用される証明書を設定して、より安全なアクセスコントロールを行うことができます。

i. **New**をクリックします。

ii. 該当するオプションを選択します。

- **Registration Key for certificate enrollment**

  証明書をアクティブにする登録キーを送信します。

  i. 登録キーの有効期限が切れる前に、ユーザが証明書をアクティベートできる日数を入力します。

  ii. **オプション:** コメントを入力します。

  iii. **オプション:** メールテンプレートをプレビューするには、**Template**をクリックします。

  iv. **Send**をクリックします。

  v. クリック**OK**でこのキーを保存します。

- **Certificate file (p12)**

  ユーザのプライベートパスワード付きの`*.p12`証明書ファイルを作成します。

  i. 証明書のパスワードを入力し、確認します。

  パスワードは、証明書ファイル内の機密データを保護するために必要です。

  ii. **オプション:** コメントを入力します。

  iii. クリック**OK**。

  iv. **Save As**ウィンドウが開くのを待ちます。

  v. **File name**フィールドでユーザ名を必ず入れます。

  vi. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

  証明書ファイルはPKCS #12形式で、拡張子は`.p12`です。

  vii. SmartConsoleコンピュータの安全な場所にアクセスします。

  viii. クリック**Save**。

  ix. このファイルとパスワードをユーザに提供します。

iii. クリック**OK**。

注:
- ユーザがしばらくシステムにアクセスしない場合(長期休暇に入るなど)、証明書を失効させることができます。これにより、ユーザアカウントは残りますが、証明書を更新するまでアクセスすることができなくなります。
- 鍵/証明書を失効させるには、鍵/証明書を選択し、**Revoke**をクリックします。

l. **Encryption** のページで次を行います。

リモートアクセスVPNのIKEv2認証と暗号化の設定を行うことができます。

i. **IKE**を選択します。

ii. クリック**Edit**。

暗号化**IKE Phase 2 Properties**ウィンドウが開きます。

iii. **Authentication**ページで、認証スキームを選択します:

i. **Password**- ユーザは事前に共有された秘密のパスワードで認証します。

ii. **Public Key**- ユーザは、証明書ファイルに含まれる公開鍵で認証を行います。

iv. **Encryption**ページで設定する項目はありません。

これらのアルゴリズムは、SmartConsole > Global プロパティ >**Remote Access** >**VPN - Authentication** > **Encryption algorithms**セクションで設定します。

v. クリック**OK**。

m. クリック**OK**。

3. **オプション: SmartConsoleのユーザ認証用にRADIUSサーバグループを設定します。**

注 - RADIUSサーバーのグループを定義する場合、グループの全メンバは同じプロトコルを使用しなければなりません。

a. SmartConsoleで、サーバグループに含めるすべてのサーバを設定します。各サーバについて、グループ内の優先順位を入力します。数字が小さいほど優先順位が高くなります。たとえば、優先度1、2、3の3台のサーバでグループを作成した場合、1番のサーバが1番目に、2番のサーバが2番目に、3番のサーバが3番目にアプローチされます。

b. サーバグループを作成します。

SmartConsole のオブジェクトエクスプローラで、**New** > **Server** > **More** > **RADIUS Group**をクリックします。

c. グループのプロパティを設定し、サーバをグループに追加します。

   i. グループに**Name**を付けます。任意の名前を選択できます。

   ii. 追加する各サーバのプラス(+) をクリックし、ドロップダウンリストから各サーバを選択します。

   iii. クリック**OK**。

   iv. SmartConsoleセッションを公開する。

d. 新しいユーザを追加します。

e. SmartConsoleセッションを公開する。

f. アクセスコントロールポリシーをインストールします。

RADIUSサーバグループを使用したユーザアクセスの許可

セキュリティゲートウェイでは、RADIUSグループへのユーザの割り当てに基づいて、認証されたRADIUSユーザのアクセス権を制御できます。これらのグループは、セキュリティポリシーの中で、ユーザに特定のリソースへのアクセスを制限したり、与えたりするために使用されます。ユーザは自分が属しているグループは知りません。

RADIUSグループを使用するには、RADIUSサーバのRADIUSユーザプロファイルにreturn属性を定義する必要があります。この属性はセキュリティゲートウェイに返され、ユーザが属するグループ名(例えば、**RAD_<RADIUSユーザが属するグループ>) を**含みます。

RADIUS属性「`Vendor-Specific`」(26)を使用します。RFC 2865を参照してください。

TACACSサーバ認証によるユーザアカウントの作成

TACACS(Terminal Access Controller Access Control System) は、1つまたは複数の集中型サーバを通じて、ルータやネットワークアクセスサーバなどのネットワーク接続デバイスのアクセス制御を行うシステムです。

TACACSは、検証サービスを提供する外部認証メソッドです。TACACSでは、リモートユーザからの認証要求をTACACSサーバに転送します。ユーザのアカウント情報を保存するTACACSサーバで、ユーザ認証が行われます。物理的なカードキーデバイスやトークンカード、Kerberosの秘密キー認証に対応しています。TACACSは、すべての認証要求のユーザ名、パスワード、認証サービス、およびアカウンティング情報を暗号化し、通信の安全性を確保します。

TACACS認証を使用するようにセキュリティゲートウェイを設定するには、サーバを設定し、セキュリティゲートウェイでTACACS認証の使用を有効にする必要があります。

ユーザは、TACACSサーバまたはTACACSサーバグループを通じてTACACS認証を実行できます。TACACSサーバグループは、同一のTACACSサーバのハイアベイラビリティグループであり、システム内の任意またはすべてのTACACSサーバを含みます。グループを作成する際に、グループ内の各サーバに優先順位を定義します。優先順位の高いサーバに障害が発生すると、グループ内で次に優先順位の高いサーバに引き継がれ、その後も同様になります。すべてのTACACSサーバに同じ優先度を割り当てると、セキュリティゲートウェイは認証のためにそのうちの1つをランダムに選択します。

TACACSサーバによる認証を構成した後、さらに証明書ファイルによる認証を構成することができます。その後、ユーザはTACACSサーバまたは証明書ファイルを使ってセキュリティゲートウェイを認証できます。

ユーザのTACACSサーバ認証を設定するには

1. SmartConsoleで、新しいTACACS / TACACS+サーバオブジェクトを設定します。
    a. 右上のObjectsパネルをクリックします。
    b. New >More >Server >TACACS をクリックします。
    c. 一番上のフィールドに、該当するオブジェクト名を入力します。
    d. オプション: コメントを入力します。
    e. Hostフィールドで、ドロップダウン矢印をクリックし、「New」をクリックします。
    f. New HostをTACACSサーバのIP addressで作成します。クリックOK。
    g. このホストがNew TACACSウィンドウのHostフィールドに表示されていることを確認します。

h. **Servers type**セクションで、該当する値を選択します。

ベストプラクティス - デフォルト値は**TACACS**ですが、**TACACS+**を推奨します。

i. **TACACS+**を選択した場合は、**Secret key**フィールドに、TACACS+ サーバで以前に定義した秘密鍵を入力します。

j. **Priority**フィールドでは、デフォルト値**1**のままにしておきます。

k. クリック**OK**。

l. SmartConsoleセッションを公開する。

2. **新規ユーザを作成し、認証方法としてTACACSを選択します。**

a. 右上の**Objects**パネルをクリックします。

b. **New** >**More** >**User/Identity** >**User** をクリックします。

New Userウィンドウが開きます。

c. 該当するユーザテンプレートを選択し、**OK**をクリックします。

d. 一番上のフィールドに、該当するオブジェクト名を入力します。

大文字と小文字を区別するユニークな文字列にしてください。

Check Point以外の認証局でユーザ証明書を生成する場合、識別名(DN)の構成要素である共通名(CN)を入力します。

例:

DN:`CN = James, O = My Organization, C = My Country`

の場合、`James`をユーザ名として入力します。

ユーザ名としてコンテナを使用する場合、コンテナにはスペースを含まず、正確に1つの文字列を含める必要があります。

e. **オプション:** コメントを入力します。

f. **General**ページで、該当する設定を行います:

- **Email address**(任意)
- **Mobile phone number**(任意)
- **Expire at**

  これは、ユーザがネットワークリソースやアプリケーションへのアクセスを許可されなくなる日付です。

  デフォルトの有効期限は**Menu** >**Global Properties** >**User Accounts** >**Expiration Date** で設定されています。

g. **Groups**ページでは、該当するユーザグループオブジェクトを選択することができます(ユーザテンプレートで設定されたものに加えて、またはその代わりに)。

h. **Authentication** のページで次を行います。

i. **Authentication method**フィールドで、**TACACS**を選択します。

ii. **TACACS server**フィールドでは、デフォルト値**Any**のままにするか、該当するTACACS サーバーオブジェクトを選択します。

重要 - 認証方式を選択しない場合は、ユーザはログインもしくはネットワークリソースを利用できません。

i. **Location** のページで次を行います。

i. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可されたソースを設定します。

これらのオブジェクトは、選択する前にすでに存在している必要があります。

ii. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可された宛先を設定します。

これらのオブジェクトは、選択する前にすでに存在している必要があります。

j. **Time** のページで次を行います。

ユーザに特定の勤務日または業務時間がある場合、そのユーザがいつアクセス認証されるかを設定できます。

- **From**および**To** - 予定勤務日の開始時刻と終了時刻を入力します。このユーザは、指定された範囲外の時刻にログインを試みた場合、認証されません。
- **Days in week**または**Daily** - ユーザがリソースを認証してアクセスできる日を選択します。このユーザは、未選択の日にログインを試みた場合、認証されません。

k. **Certificates** のページで次を行います。

このユーザに適用される証明書を設定して、より安全なアクセスコントロールを行うことができます。

i. **New**をクリックします。

ii. 該当するオプションを選択します。

- **Registration Key for certificate enrollment**

  証明書をアクティブにする登録キーを送信します。

  i. 登録キーの有効期限が切れる前に、ユーザが証明書をアクティベートできる日数を入力します。

  ii. **オプション:** コメントを入力します。

  iii. **オプション:** メールテンプレートをプレビューするには、**Template**をクリックします。

  iv. **Send**をクリックします。

  v. クリック**OK**このキーを保存します。

- **Certificate file (p12)**

  ユーザのプライベートパスワード付きの`*.p12`証明書ファイルを作成します。

  i. 証明書のパスワードを入力し、確認します。

  パスワードは、証明書ファイル内の機密データを保護するために必要です。

  ii. **オプション:** コメントを入力します。

  iii. クリック**OK**。

  iv. **Save As**ウィンドウが開くのを待ちます。

  v. **File name**フィールドに、ユーザ名を必ず入れます。

  vi. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

  証明書ファイルはPKCS #12形式で、拡張子は`.p12`です。

  vii. SmartConsoleコンピュータの安全な場所にアクセスします。

  viii. クリック**Save**。

  ix. ユーザにこのファイルとパスワードを渡します。

iii. クリック**OK**。

注:
- ユーザがしばらくシステムにアクセスしない場合(長期休暇に入るなど)、証明書を失効させることができます。これにより、ユーザアカウントは残りますが、証明書を更新するまでアクセスすることができなくなります。
- 鍵/証明書を失効させるには、鍵/証明書を選択し、**Revoke**をクリックします。

l. **Encryption** のページで次を行います。

リモートアクセスVPNのIKEv2認証と暗号化の設定を行うことができます。

i. **IKE**を選択します。

ii. クリック**Edit**。

暗号化**IKE Phase 2 Properties**ウィンドウが開きます。

iii. **Authentication**ページで、認証スキームを選択します:

i. **Password**- ユーザは事前に共有された秘密のパスワードで認証します。

ii. **Public Key**- ユーザは、証明書ファイルに含まれる公開鍵で認証を行います。

iv. **Encryption**ページで設定する項目はありません。

これらのアルゴリズムは、SmartConsole > Global プロパティ >**Remote Access** >**VPN - Authentication** > **Encryption algorithms**セクションで設定します。

v. クリック**OK**。

m. クリック**OK**。

3. **オプション: SmartConsoleのユーザ認証用にTACACSサーバグループを設定します。**

注 - TACACSサーバのグループを定義する場合、グループの全メンバは同じプロトコルを使用する必要があります。

a. SmartConsoleで、サーバグループに含めるすべてのサーバを設定します。

各サーバについて、グループ内の優先順位を入力します。数字が小さいほど優先順位が高くなります。

たとえば、優先度1、2、3の3台のサーバでグループを作成した場合、1番のサーバが1番目に、2番のサーバが2番目に、3番のサーバが3番目にアプローチされます。

b. サーバグループを作成します。

SmartConsole のオブジェクトエクスプローラで、**New** > **Server** > **More** > **TACACS Group**をクリックします。

c. グループのプロパティを設定し、サーバをグループに追加します。

   i. グループに**Name**を付けます。任意の名前を選択できます。

   ii. 追加する各サーバのプラス(+) をクリックし、ドロップダウンリストから各サーバを選択します。

   iii. クリック**OK**。

   iv. SmartConsoleセッションを公開する。

d. 新しいユーザを追加します。

e. SmartConsoleセッションを公開する。

f. アクセスコントロールポリシーをインストールします。

SecurID認証によるユーザアカウントの作成

SecurIDは、ユーザがトークン認証デバイスを所有し、PINまたはパスワードを提供することを要求します。トークン認証は、RSA認証マネージャ(AM) に同期するワンタイムパスワードを生成するもので、ハードウェアまたはソフトウェアの形態で提供されます。ハードウェアトークンは、キーホルダーやクレジットカード大のデバイスです。ソフトウェアトークンは、ユーザが認証を希望するPCやデバイスに置かれます。すべてのトークンは、約1分ごとに変化するランダムな1回限りのアクセスコードを生成します。ユーザが保護されたリソースに対して認証を試みる場合、AMによってワンタイムのコードが検証される必要があります。

セキュリティゲートウェイは、リモートユーザによる認証要求をAMに転送します。AMは、RSAユーザのデータベースと、割り当てられたハードトークンまたはソフトトークンを管理します。セキュリティゲートウェイはAMエージェントとして機能し、すべてのアクセス要求をAMに送り認証します。エージェント構成の詳細については、RSA Authentication Managerのドキュメントを参照してください。SecurID認証方式に必要なパラメータは特にありません。認証リクエストは、SDKがサポートするAPIまたはREST APIを介して送信できます。

SecurID認証を設定した後、さらに証明書ファイルによる認証を設定できます。その後、ユーザはSecurIDまたは証明書ファイルを使ってセキュリティゲートウェイを認証できます。

ユーザにSecurID認証を設定するには

1. **認証リクエストを送信するAPIを設定する**

   2つのAPIタイプのうち、いずれかを選択して有効にすることができます。

■ **SDKがサポートするAPI**

特定のプラットフォームで利用可能なSDKを通じて、UDPポート5500で独自の通信プロトコルを使用する独自のAPI。

SDKがサポートするAPI上でSecurID認証を有効にするには

a. ACE/サーバで`sdconf.rec`ファイルを作成し、コンピュータにコピーします。

詳細はRSAのドキュメントを参照。

重要 - ACE/サーバに接続するセキュリティゲートウェイインタフェースのIPアドレスを使用します。

- **特定のセキュリティゲートウェイの場合**
  IPアドレスを認証エージェントとして設定します。
- **クラスタの場合**
  これらのIPアドレスを認証エージェントとして設定します：各クラスタメンバの物理IPアドレスとクラスタ仮想IPアドレス。
- **特定のVSXゲートウェイ上のVSXバーチャルシステムの場合**
  以下のIPアドレスを認証エージェントとして設定：VSXゲートウェイのIPアドレスと仮想システムのIPアドレス。
- **VSXクラスタ上のVSX仮想システムの場合**
  以下のIPアドレスを認証エージェントとして設定する：VSXクラスタのクラスタ仮想IPアドレスと仮想システムのクラスタ仮想IPアドレス。

b. SmartConsoleでSecurIDオブジェクトを開き、**参照**をクリックして、`sdconf.rec`ファイルをSecurIDオブジェクトにインポートします。

c. アクセスコントロールポリシーをインストールします。

注 - ポリシーのインストール中に、`sdconf.rec`ファイルがセキュリティゲートウェイから`/var/ace/sdconf.rec`に転送されます。

- **REST API**

  REST API上でSecurID認証を有効にするには

  a. Security Groupでコマンドラインに接続します。

  b. エキスパートモードにログインします。

  c. VSXゲートウェイまたはVSXクラスタメンバで、VSID 0のコンテキストに移動します。

  ```
  vsenv 0
  ```

  d. 現在の`$CPDIR/conf/RSARestServer.conf`ファイルをバックアップします。

  ```
  cp -v $CPDIR/conf/RSARestServer.conf{,_BKP}
  ```

  e. `$CPDIR/conf/RSARestServer.conf`ファイルを編集します。

  ```
  vi $CPDIR/conf/RSARestServer.conf
  ```

  次のフィールドに入力します。

  - `host`- 設定されているRSAサーバのホスト名。
  - `port`、`client key`、`accessid` - RSA SecurID Authentication APIウィンドウから。
  - `certificate`- 証明書ファイルの名前。

  f. 変更内容をファイルに保存し、エディタを終了します。

注 - REST APIの設定を完了しない場合、認証はSDKがサポートするAPIを介して行われます。

2. **ユーザグループの設定**

   a. SmartConsoleで、オブジェクトエクスプローラ(F11)を開きます。

   b. **New >More >User/Identity >User Group** をクリックします。

   New User Groupウィンドウが開きます。

   c. グループ名を入力します。

   例：`SecurID_Users`

   グループが空であることを確認します。

   d. クリック**OK**。

   e. SmartConsoleセッションを公開する。

   f. アクセスコントロールポリシーをインストールします。

3. **新規ユーザを作成し、認証方法としてSecurIDを定義します。**

   この設定手順は、内部ユーザ(SmartConsoleで定義) と外部ユーザで異なります。

   内部ユーザのSecurID認証設定を行うには

   内部ユーザとは、SmartConsoleで設定したユーザのことです。Security Management Serverは、これらのユーザを管理データベースに保持します。

   a. SmartConsoleで、オブジェクトエクスプローラ(F11)を開きます。

   b. **New** >**More** >**User/Identity** >**User**をクリックします。

      New Userウィンドウが開きます。

   c. 該当するユーザテンプレートを選択し、**OK**をクリックします。

   d. 一番上のフィールドに、該当するオブジェクト名を入力します。

      大文字と小文字を区別するユニークな文字列にしてください。

      Check Point以外の認証局でユーザ証明書を生成する場合、識別名(DN) の構成要素である共通名(CN) を入力します。

      例:

      DN:`CN = James, O = My Organization, C = My Country`

      `James`をユーザ名として入力します。

      ユーザ名としてコンテナを使用する場合、コンテナにはスペースを含まず、正確に1つの文字列を含める必要があります。

   e. **オプション:** コメントを入力します。

   f. **General**ページで、該当する設定を行います:

      - **Email address**(任意)
      - **Mobile phone number**(任意)
      - **Expire at**

        これは、ユーザがネットワークリソースやアプリケーションへのアクセスを許可されなくなる日付です。

   g. **Groups**ページでは、該当するユーザグループオブジェクトを選択することができます(ユーザテンプレートで設定されたものに加えて、またはその代わりに) 。

   h. **Authentication**ページで、**Authentication method**フィールドで、**SecurID**を選択します。

i. **Location** のページで次を行います。

   i. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可されたソースを設定します。

      これらのオブジェクトは、選択する前にすでに存在している必要があります。

   ii. このユーザがデータおよびトラフィックにアクセスまたは送信できる許可された宛先を設定します。

      これらのオブジェクトは、選択する前にすでに存在している必要があります。

j. **Time** のページで次を行います。

   ユーザに特定の勤務日または業務時間がある場合は、そのユーザがいつアクセス認証されるかを設定できます。

   - **From**および**To** - 予定勤務日の開始時刻と終了時刻を入力します。指定された範囲外の時間にログインが試みられた場合、このユーザは認証されません。
   - **Days in week**または**Daily** - ユーザがリソースを認証してアクセスできる日を選択します。このユーザは、未選択の日にログインを試みた場合、認証されません。

k. **Certificates** のページで次を行います。

   このユーザに適用される証明書を設定して、より安全なアクセスコントロールを行うことができます。

i. **New**をクリックします。

ii. 該当するオプションを選択します。

- **Registration Key for certificate enrollment**

  証明書をアクティブにする登録キーを送信します。

  i. 登録キーの有効期限が切れる前に、ユーザが証明書をアクティベートできる日数を入力します。

  ii. **オプション:** コメントを入力します。

  iii. **オプション:** メールテンプレートをプレビューするには、**Template**をクリックします。

  iv. **Send**をクリックします。

  v. クリック**OK**このキーを保存します。

- **Certificate file (p12)**

  ユーザのプライベートパスワード付きの`*.p12`証明書ファイルを作成します。

  i. 証明書のパスワードを入力し、確認します。

  パスワードは、証明書ファイル内の機密データを保護するために必要です。

  ii. **オプション:** コメントを入力します。

  iii. クリック**OK**。

  iv. **Save As**ウィンドウが開くのを待ちます。

  v. **File name**フィールドにユーザ名を必ず入れます。

  vi. **Save as type**フィールドで、**Certificate Files (*p12)**を選択します。

  証明書ファイルはPKCS #12形式で、拡張子は`.p12`です。

  vii. SmartConsoleコンピュータの安全な場所にアクセスします。

  viii. クリック**Save**。

  ix. このファイルとパスワードをユーザに提供します。

iii. クリック**OK**。

注：

- ユーザがしばらくシステムにアクセスしない場合（長期休暇に入るなど）、証明書を失効させることができます。これにより、ユーザアカウントは残りますが、証明書を更新するまでアクセスすることができなくなります。
- 鍵/証明書を失効させるには、鍵/証明書を選択し、**Revoke**をクリックします。

l. **Encryption** のページで次を行います。

リモートアクセスVPNのIKEv2認証と暗号化の設定を行うことができます。

i. **IKE**を選択します。

ii. クリック**Edit**。

暗号化**IKE Phase 2 Properties**ウィンドウが開きます。

iii. **Authentication**ページで、認証スキームを選択します：

i. **Password**- ユーザは事前に共有された秘密のパスワードで認証します。

ii. **Public Key**- ユーザは、証明書ファイルに含まれる公開鍵で認証を行います。

iv. **Encryption**ページで設定する項目はありません。

これらのアルゴリズムは、SmartConsole > Global プロパティ >**Remote Access** >**VPN - Authentication** > **Encryption algorithms**セクションで設定します。

v. クリック**OK**。

m. クリック**OK**。

外部ユーザのSecurID認証設定を行うには

外部ユーザとは、Legacy SmartDashboardを構成するユーザです。

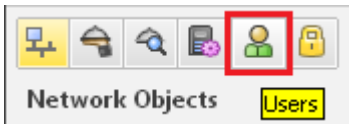
Security Management Serverは、これらのユーザを管理データベースに保持しません。

a. SmartConsole で、**Manage & Settings** > **Blades**をクリックします。

b. **Mobile Access**セクションで、**Configure in SmartDashboard**をクリックします。

レガシーSmartDashboardが開きます。

c. 左下のNetwork Objectsペインで、Usersをクリックします。



d. 空いているスペースで右クリックし、該当するオプションを選択します。

- 外部認証スキームを1つだけサポートする場合は、**New > External User Profile > Match all users**をクリックします。
- 複数の外部認証スキームをサポートしている場合は、**New > External User Profile > Match by domain**をクリックします。

e. **External User Profile**のプロパティを設定します。

i. **General Properties** のページで次を行います。

- **Match all users**を選択した場合、次のように設定します。
  - **External User Profile name**フィールドで、デフォルトの名前`generic*`をそのままにしておきます。
  - **Expiration Date**フィールドに、該当する日付を設定します。
- **Match by domain**を選択した場合、次のように設定します。
  - **External User Profile name**フィールドに、該当する名前を入力します。この名前は、認証マネージャがユーザを認証するために使用されます。
  - **Expiration Date**フィールドに、該当する日付を設定します。
  - **Domain Name matching definitions**セクションで、該当する設定を行います。

ii. **Authentication** のページで次を行います。

Authentication Schemeドロップダウンリストから、**SecurID**を選択します。

iii. クリック**OK**。

f. 上部のツールバーから、**Update**をクリックします(または**CTRL S**キーを押す) 。

g. レガシーSmartDashboardを閉じます。

4. **SecurID認証の設定を完了する**

a. アドレス変換ルールベースで、セキュリティゲートウェイとAuthentication Manager間の接続がNAT処理されていないことを確認します。

VSXバーチャルシステムでは、sk107281の指示に従います。

b. SmartConsoleで、Access Controlポリシーをインストールします。

セキュリティゲートウェイに複数のインタフェースがある場合、セキュリティゲートウェイ上のSecurIDエージェントが認証マネージャからの応答を復号する際に誤ったインタフェースIPを使用し、認証に失敗することがありました。

この問題を解決するには、`sdopts.rec`という名前の新しいテキストファイルを、`sdconf.rec`と同じディレクトリに置きます。

ファイル`sdopts.rec`に次の行を含めます:

```
CLIENT_IP=<IP Address>
```

ここでの*<IP Address>*は、Authentication Managerで定義されたセキュリティゲートウェイのプライマリIPアドレスです。サーバのルーティング先となるインタフェースのIPアドレスとなります。

例:

```
CLIENT_IP=192.168.20.30
```

注 - VSXゲートウェイとVSXクラスタメンバでは、VSID 0のコンテキストと該当する各仮想システムのコンテキストで、同じ`sdopts.rec`ファイルを作成する必要があります。

アクセスロール

アクセスロールオブジェクトによって、ネットワークアクセスを設定することができます:

- ネットワーク
- ユーザとユーザグループ
- コンピュータとコンピュータグループ
- リモートアクセスVPNクライアント(セキュリティゲートウェイR80.10以降に対応)

Identity Awareness Software Bladeを有効にすると、アクセスロールオブジェクトを作成し、アクセスコントロールポリシールールの**Source**と**Destination**カラムで使用できます。

詳細は次を参照: *R82 Identity Awareness Administration Guide*。

アクセスロールの追加

重要 - Active Directoryのユーザ、マシン、またはグループをアクセスロールに追加する前に、Security Management Serverと管理ディレクトリを保持するADサーバの間にLDAP接続があることを確認してください。管理ディレクトリは、**LDAP Account Unit** の**Properties**ウィンドウの**Objects Management**タブで定義します。

アクセスロールを作成するには

1. オブジェクトツリーで、**New> More > Users > Access Role**をクリックします。

   New Access Roleウィンドウが開きます。
2. アクセスロールに**Name**を入力します。
3. **Comment**を入力します(オプション)。
4. オブジェクトの**Color**を選択します(オプション)。
5. **Networks**ペインで、以下のいずれかを選択します。
   - **Any network**
   - **Specific networks**- 各ネットワークについて、**+**をクリックし、リストからネットワークを選択します。
6. **Users**ペインで、以下のいずれかを選択します。
   - **Any user**
   - **All identified users**- サポートされている認証方法(内部ユーザ、Active Directoryユーザ、またはLDAPユーザ)によって識別されるすべてのユーザが含まれます。

- **Specific users/groups**- 各ユーザまたはユーザグループについて、**+**をクリックし、リストからユーザまたはグループを選択します。

7. **Machines**ペインで、以下のいずれかを選択します。
   - **Any machine**
   - **All identified machines**- サポートされている認証方法(Active Directory)によって識別されたマシンが含まれます。
   - **Specific machines**- 各マシンについて、**+**をクリックし、リストからマシンを選択します。
8. **Remote Access Clients**ペインで、リモートアクセス用のクライアントを選択します。
9. クリック**OK**。

アイデンティティアウェアネスエンジンは、LDAPグループメンバシップの変更を自動的に認識し、アクセスロールを含むアイデンティティ情報を更新します。

ユーザディレクトリ

Check Pointユーザディレクトリには、ユーザ固有の情報が保存されます。

注 - User Directoryは特別なライセンスが必要です。Mobile Access Software Bladeをお持ちの方は、ユーザディレクトリのライセンスを持っています。

ユーザディレクトリでは、次のことが可能です:

- *ハイアベイラビリティ*を設定し、ユーザデータを複数のサーバに複製してバックアップする。

  参照: *アカウントユニットとハイアベイラビリティ (215ページ)*。

- 分散データベース用に*複数のアカウントユニット*を設定する。
- 暗号化されたユーザディレクトリ接続用に、*LDAPアカウントユニットを定義*する。

  参照: *LDAPサーバの変更 (215ページ)*。

- 複数のLDAPベンダーをサポートするために*プロファイル*を設定する。

  参照: *ユーザディレクトリのプロファイル (191ページ)*。

ユーザディレクトリに関する考察

始める前に、ユーザディレクトリの使用計画を立ててください。

- ユーザディレクトリサーバを、ユーザ管理、CRL検索、ユーザ認証、またはこれらすべてのいずれに使用するかを決定する。

  参照: *LDAPアカウント単位での作業 (209ページ)*。

- 必要なアカウントユニットの数を決定する。

  ユーザディレクトリサーバごとに用意することもできますし、1つのユーザディレクトリサーバのブランチを異なるアカウントユニットに分割することもできます。

  参照: *アカウントユニット (209ページ)*。

- ハイアベイラビリティ設定を使用するかどうかを決定する。

  参照: *アカウントユニットとハイアベイラビリティ (215ページ)*。

- ハイアベイラビリティとクエリを目的としたユーザディレクトリサーバ間の優先順位を決定します。

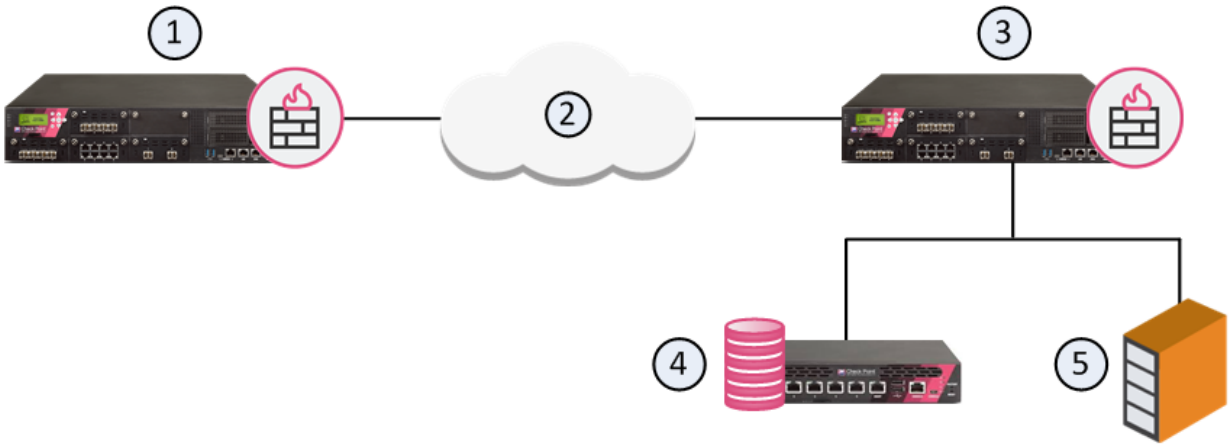
  参照: *ハイアベイラビリティ優先度の設定 (216ページ)*。

- ユーザを異なるアカウントユニット、ブランチ、サブブランチに割り当て、共通の属性(組織におけるロール、権限など)を持つユーザをグループ化します。

  参照: *ユーザディレクトリサーバでのユーザ管理 (204ページ)*。

ユーザディレクトリの展開

ユーザディレクトリは、Security Management ServerとLDAPサーバを統合し、セキュリティゲートウェイにLDAPの情報を使用させます。



項目	説明
1	セキュリティゲートウェイ - LDAPユーザ情報とCRLを取得
2	インターネット
3	セキュリティゲートウェイ - LDAPユーザ情報の照会、CRLの取得、認証のためのバインド操作
4	Security Management Server - ユーザディレクトリを使用してユーザ情報を管理
5	LDAPサーバ - 1つ以上のアカウントユニットを保持するサーバ

ユーザディレクトリの有効化

SmartConsoleで、Security Management Serverを有効にして、アカウントユニットのユーザを管理します。参照: *LDAPアカウント単位での作業 (209ページ)*。

注 - ユーザディレクトリLDAPサーバが有効な場合、SmartConsoleユーザデータベースを使用することはできません。

Security Management Serverでユーザディレクトリを有効にするには

1. メニューから、**Global Properties** >**User Directory** を選択します。

   User Directoryページが開きます。

2. **Use User Directory for Security Gateways**を選択します。
3. ログインとパスワードを設定します。
4. クリック**OK**。
5. **Gateways & Servers**ビュー(Ctrl+1) で、編集用にSecurity Management Serverオブジェクトを開きます。
6. **General Properties**ページの**Management**タブで、**Network Policy Management**と**User Directory**を選択します。
7. クリック**OK**。
8. ポリシーをインストールします。

LDAP用ユーザディレクトリスキーマ

ユーザディレクトリのデフォルトスキーマは、ユーザディレクトリのデータの構造の記述です。

LDAPサーバのユーザ定義が定義されています。

このスキーマには、IKE関連の属性、認証方法、リモートユーザの値など、Security Management ServerやSecurity Gateway固有のデータは含まれていません。

すべてのユーザが同じ認証方法を持ち、デフォルトのテンプレートに従って定義されている場合、デフォルトのユーザディレクトリスキーマを使用することができます。

しかし、データベース内のユーザの定義が異なる場合は、LDAPサーバにCheck Pointのスキーマを適用した方がよいでしょう。

参照: *LDAP用ユーザディレクトリスキーマ (181ページ)*。

Check Pointスキーマは、LDAPサーバ内の構造にSecurity Management Serverおよびセキュリティゲートウェイ固有のデータを追加します。

Check Pointスキーマを使用して、ユーザ認証機能を持つオブジェクトの定義を拡張することができます。

たとえば、**fw1Person**というオブジェクトクラスは、Check Pointスキーマの一部です。

このオブジェクトクラスには、Person属性の定義に追加するための必須属性とオプション属性があります。

他の例としては、**fw1Template**があります。これは、ユーザ情報のテンプレートを定義する独立した属性です。

スキーマチェック

スキーマチェックを有効にすると、ユーザディレクトリは、すべてのCheck Pointのオブジェクトクラスとその関連属性がディレクトリスキーマに定義されていることを要求します。

ユーザディレクトリで作業する前に、スキーマチェックが無効になっていることを確認してください。そうでない場合、統合は失敗します。

Check Pointのオブジェクトクラスと属性をユーザディレクトリサーバのスキーマに適用した後、スキーマチェックを再度有効にする必要があります。

OID専用属性

独自のオブジェクトクラスと属性(すべて"`fw1`"で始まる)には、それぞれ以下に示す独自のオブジェクト識別子(OID)が設定されています。

オブジェクトクラスOID

オブジェクトクラス	OID
fw1template	1.3.114.7.4.2.0.1
fw1person	1.3.114.7.4.2.0.2

独自属性のOIDは、同じプレフィックスで始まります("1.3.114.7.4.2.0.X")。

"X"の値だけが各属性で異なります。

参照: *ユーザディレクトリスキーマ属性 (182ページ)*。

ユーザディレクトリスキーマ属性

cn

エントリーの名前。

「Common Name(コモンネーム)」とも言います。

ユーザの場合は、セキュリティゲートウェイへのログインに使用される名前であるuid属性と異なる場合があります。

この属性は、ユーザディレクトリエントリの識別名、つまりDNのRDNを構築するためにも使用されます。

uid

ユーザのログイン名、つまりセキュリティゲートウェイにログインする際に使用する名前。

この属性は、「内部パスワード」を除くすべての認証方式で外部認証システムに渡され、これらの認証方式すべてで定義する必要があります。

ログイン名は、Security Management ServerがUser Directoryサーバ(複数可)を検索するために使用されます。

このため、各ユーザエントリは一意のUID値を持つ必要があります。

フルパスのDNを使用してセキュリティゲートウェイにログインすることもできます。

DNは、この属性に曖昧さがある場合、または"内部パスワード"でこの属性が欠落している可能性がある場合に使用することができます。

DNは、同じユーザ(同じuid)が異なるUser Directoryサーバ上の複数のアカウントユニットに定義されている場合にも使用することができます。

description

ユーザに関する説明テキスト。

デフォルトは"no value"です。

メール

ユーザのEメールアドレス。

デフォルトは"no value"です。

member

エントリには、この属性の値を0個以上指定することができます。

- **テンプレート内:** このテンプレートを使用するユーザエントリのDN。ユーザでないDN(オブジェクトクラスが"person"、"organizationalPerson"、"inetOrgPerson"、"fw1person"のいずれかでないもの)は無視されます。
- **グループ内:** ユーザのDN。

userPassword

認証方法(fw1auth-method)が"Internal Password"の場合に必ず指定します。この値は"crypt"を用いてハッシュ化できます。この場合、この属性の構文は次のようになります。

"{crypt}xxyyyyyyyyyy"

この場合:

- "xx"は"salt"です。
- "yyyyyyyyyy"はハッシュ化されたパスワード

ハッシュ化せずにパスワードを保存することも可能です(推奨しません) 。ただし、User Directoryサーバでハッシュ化を指定している場合は、パスワードの二重ハッシュ化を防ぐため、ここではハッシュ化を指定しないようにします。この場合、暗号化されていないパスワードの送信を防ぐために、SSLを使用する必要があります。

セキュリティゲートウェイはこの属性を書き込むことはあっても、読み込むことはありません。その代わり、ユーザディレクトリのバインド操作でパスワードの検証を行います。

fw1authmethod

いずれかの方法を実行します。

- RADIUS
- TACACS
- SecurID
- OSパスワード
- Defender

この属性のデフォルト値は、SmartConsoleの**Account Unit**ウィンドウの**Authentication**タブにある**Default authentication scheme**で上書きされます。

たとえば、User Directoryサーバでは、サーバのスキーマに独自のオブジェクトクラス"fw1person"が追加されていないにもかかわらず、すべてのオブジェクトクラス"person"のUser Directoryエントリが含まれていることがあります。

SmartConsoleの**Default authentication scheme**が「内部パスワード」の場合、すべてのユーザは"userPassword"属性に保存されているパスワードを使用して認証されます。

fw1authserver

OIDの"X"	fw1person	fw1template	デフォルト
1	y	y	"未定義"

認証を行うサーバの名前。

このフィールドは、fw1auth-method が "RADIUS"または"TACACS"の場合に指定する必要があります。

他のすべてのfw1auth-methodの値については、無視されます。意味は以下の通りです。

方法	意味
RADIUS	RADIUSサーバの名前、RADIUSサーバのグループ、または「Any」

方法	意味
TACACS	TACACSサーバの名前

OIDの"X"	fw1template
2	y

fw1pwdLastMod

パスワードが最後に変更された日付。

フォーマットは`yyyymmdd`(例:1998年8月20日は19980820)です。

パスワードは、認証プロセスの一部として、セキュリティゲートウェイを通じて変更することができます。

OIDの"X"	fw1person	fw1template	デフォルト
3	y	y	値がない場合は、パスワードは一度も変更されたことがない。

fw1expiration-date

ユーザがセキュリティゲートウェイにログインできる最後の日付。有効期限がない場合は"値なし"。

フォーマットは`yyyymmdd`(例:1998年8月20日は19980820)です。

デフォルトは"`no value`"です。

OIDの"X"	fw1person	fw1template	デフォルト
8	y	y	"値なし"

fw1hour-range-from

ユーザがセキュリティゲートウェイにログインできるようになる時間。

フォーマットは`hh:mm`(例:午前8時15分は08:15)です。

OIDの"X"	fw1person	fw1template	デフォルト
9	y	y	"00:00"

fw1hour-range-to

ユーザがセキュリティゲートウェイにログインできるまでの時間。

フォーマットは`hh:mm`(例:午前8時15分は08:15)です。

OIDの"X"	fw1person	fw1template	デフォルト
10	y	y	"23:59"

fw1day

ユーザがセキュリティゲートウェイにログインできる日(曜日)。

値は"`SUN`"、"`MON`"などと指定可能。

OIDの"X"	fw1person	fw1template	デフォルト
11	y	y	全曜日

fw1allowed-src

ユーザがクライアントを実行できる1つ以上のネットワークオブジェクトの名前。この制限を解除するには"`Any`"、そのようなクライアントが存在しない場合は"`no value`"。

Security Management Serverで定義されたネットワークオブジェクトの名前と一致する必要があります。

OIDの"X"	fw1person	fw1template	デフォルト
12	y	y	"値なし"

fw1allowed-dst

ユーザがアクセスできる1つまたは複数のネットワークオブジェクトの名前。この制限を解除するには"`Any`"、そのようなネットワークオブジェクトがない場合は"`no value`"。

この名前は、Security Management Serverで定義されたネットワークオブジェクトの名前と一致する必要があります。

OIDの"X"	fw1person	fw1template	デフォルト
13	y	y	"値なし"

fw1allowed-vlan

現在は使用していません。

OIDの"X"	fw1person	fw1template	デフォルト
14	y	y	"値なし"

fw1SR-keym

SecuRemoteでセッションキーを暗号化するために使用されるアルゴリズム。

CLEAR"、"FWZ1"、"DES"、"Any"のいずれかを指定できます。

OIDの"X"	fw1person	fw1template	デフォルト
15	y	y	"Any"

fw1SR-datam

SecuRemoteでデータの暗号化に使用するアルゴリズム。

CLEAR"、"FWZ1"、"DES"、"Any"のいずれかを指定できます。

OIDの"X"	fw1person	fw1template	デフォルト
16	y	y	"Any"

fw1SR-mdm

SecuRemoteのデータへの署名に使用されるアルゴリズム。

none"または"MD5"を指定できます。

OIDの"X"	fw1person	fw1template	デフォルト
17	y	y	"なし"

fw1enc-fwz-expiration

SecuRemoteユーザがセキュリティゲートウェイに対して再認証を行う必要がある時間 (分)。

OIDの"X"	fw1person	fw1template
18	y	y

fw1sr-auth-track

SecuRemoteによる認証に成功した場合に発生する例外。

none"、"cryptlog"、"cryptalert"のいずれかを指定できます。

OIDの"X"	fw1person	fw1template	デフォルト
19	y	y	"なし"

fw1groupTemplate

このフラグは、グループメンバシップに関連する問題を解決するために使用します。

ユーザのグループメンバーシップは、そのユーザが属するグループエントリ、ユーザエントリ自身、またはその両方のエントリに保存されます。

そのため、グループ関係についてテンプレートからの情報を使用すべきかどうか、ユーザエントリでは明確ではありません。

このフラグが"TRUE"の場合、ユーザはテンプレートが属するすべてのグループのメンバとみなされます。

これは、ユーザが直接メンバになっているすべてのグループに追加されます。

OIDの"X"	fw1person	fw1template	デフォルト
20	y	y	"False"

fw1ISAKMP-EncMethod

IKEを使用するSecuRemoteユーザの鍵暗号化方式。

これは、1つまたは複数の"DES"や"3DES"にすることができます。

IKE(旧称:ISAMP)を使用するユーザは、両方の方法を定義することができます。

OIDの"X"	fw1person	fw1template	デフォルト
21	y	y	"DES"、"3DES"

fw1ISAKMP-AuthMethods

IKE(旧ISAMP)を使用するSecuRemoteユーザに許可される認証方法です。

これは、1つまたは複数の"preshared"や"signatures"にすることができます。

OIDの"X"	fw1person	fw1template	デフォルト
22	y	y	"signatures"

fw1ISAKMP-HashMethods

IKE(旧ISAMP)を使用するSecuRemoteユーザのためのデータ整合性方式です。

これは、1つまたは複数の"MD5"や"SHA1"にすることができます。

IKEを使用するユーザは、両方の方式を定義しておく必要があります。

OIDの"X"	fw1person	fw1template	デフォルト
23	y	y	"MD5", "SHA1"

fw1ISAKMP-Transform

IKE(旧ISAMP) を使用したSecuRemoteユーザ向けのIPSec Transform方式です。

これは、"AH"または"ESP"のいずれかになります。

OIDの"X"	fw1person	fw1template	デフォルト
24	y	y	"ESP"

fw1ISAKMP-DataIntegrityMethod

IKE(旧ISAMP) を使用するSecuRemoteユーザのためのデータ整合性方式です。

これは、"MD5"または"SHA1"のいずれかになります。

OIDの"X"	fw1person	fw1template	デフォルト
25	y	y	"SHA1"

fw1ISAKMP-SharedSecret

IKE(旧ISAMP) を使用するSecuRemoteユーザの事前共有秘密キーです。

この値は、fw ikecrypt コマンドラインを使用して計算できます。

OIDの"X"	fw1person	fw1template
26	y	y

fw1ISAKMP-DataEncMethod

fw1ISAKMP-DataEncMethod

IKE(旧ISAMP) を使用したSecuRemoteユーザのデータ暗号化方式です。

OIDの"X"	fw1person	fw1template	デフォルト
27	y	y	"DES"

fw1enc-Methods

SecuRemoteユーザに許可された暗号化方式です。

これは、"FWZ"、"ISAKMP"(IKEを意味する) のうちの1つ以上にすることができます。

OIDの"X"	fw1person	fw1template	デフォルト
28	y	y	"FWZ"

fw1userPwdPolicy

パスワードをいつ、誰が変更すべきかを定義します。

OIDの"X"	fw1person
29	y

fw1badPwdCount

間違ったパスワードを連続して入力できる回数。

OIDの"X"	fw1person
30	y

fw1lastLoginFailure

最後にログインが失敗した時刻。

OIDの"X"	fw1person
31	4

memberof template

ユーザが属するテンプレートのDN。

OIDの"X"	fw1person
33	4

Netscape LDAPスキーマ

Netscapeのディレクトリサーバに適切なスキーマを追加するには、
`$FWDIR/lib/ldap/schema.ldif`ファイルを使用します。

重要 - これにより、スキーマからオブジェクトクラスの定義が削除され、更新されたものがその場所に追加されます。

コマンドを実行する前に、ユーザディレクトリサーバをバックアップしておくことをお勧めします。

`ldif`ファイル:

- スキーマに新しい属性を追加
- 古い定義を削除(`fw1person`、`fw1template`
- 新しい定義を追加(`fw1person`、`fw1template`

Netscape LDAPスキーマを変更するには、**schema.ldif**ファイルを指定して、**ldapmodify**コマンドを実行します。

注 - サーバのバージョンによっては、`delete objectclass`の操作に成功しても、エラーが返されることがあります。`ldapmodify`を`-c` (連続)オプションで使用します。

ユーザディレクトリのプロファイル

ユーザディレクトリプロファイルは、より正確なユーザディレクトリの要求を定義し、サーバとの通信を強化するための設定可能なLDAPポリシーです。

プロファイルは、LDAP サーバ固有の知識のほとんどを制御します。異なるベンダーのLDAPサーバを統合するために、多様な技術的ソリューションを管理することができます。

ユーザディレクトリプロファイルを使用して、Security Management Serverのユーザ管理属性が、関連するLDAPサーバに対して正しいものであることを確認します。

たとえば、認定されたOPSECユーザディレクトリサーバがある場合、OPSEC_DSプロファイルを適用して、強化されたOPSEC固有の属性を得ることができます。

LDAPサーバには、異なるオブジェクトリポジトリ、スキーマ、オブジェクト関係があります。

- 組織のユーザデータベースには、特定のアプリケーションのために、従来とは異なるオブジェクトタイプや関係が含まれる場合があります。
- アプリケーションによっては、ユーザオブジェクトのRDN(Relatively Distinguished Name) の`cn`属性を使用するものもあれば、`uid`を使用するものもあります。
- Microsoft Active Directoryでは、ユーザ属性`memberOf`はユーザが属するグループを記述しますが、標準的なLDAPの方法では、グループオブジェクト自体に`member`属性を定義します。
- サーバによって、パスワードの保存形式が異なります。
- v3と見なされる一部のサーバには、すべてのv3仕様を実装していないものもあります。これらのサーバではスキーマを拡張できません。
- LDAPサーバには、特定のユーザデータのサポートが組み込まれているものもあれば、Check Pointスキーマ拡張属性が必要なものもあります。

たとえば、Microsoft Active Directoryには`accountExpires`というユーザ属性がありますが、その他のサーバではCheck Pointの定義する`fw1person`オブジェクトクラスの一部である`fw1expirationdate`という属性が必要です。

- サーバによっては、未定義タイプのクエリを許可するものもあれば、許可しないサーバもあります。

デフォルトのユーザディレクトリプロファイル

これらのプロファイルは、デフォルトで定義されています。

- **OPSEC_DS** - 標準的なOPSEC認定ユーザディレクトリのデフォルトプロファイル。
- **Netscape_DS** - Netscape Directory Serverのプロファイル。
- **Novell_DS** - Novell Directory Serverのプロファイル。
- **Microsoft_AD** - Microsoft Active Directoryのプロファイル。

ユーザディレクトリプロファイルの変更

プロフィールには次の主要なカテゴリがあります。

- **Common(共通)** - ユーザディレクトリへの書き込み/読み取りのためのプロファイル設定。
- **Read(読み取り)** - ユーザディレクトリから読み取り専用のプロファイル設定。
- **Write(書き込み)** - ユーザディレクトリへの書き込み専用のプロファイル設定。

これらのカテゴリの中には、サーバが操作の種類に応じて動作するように、同じエントリを異なる値でリストアップするものがあります。デフォルトのプロファイルの特定のパラメータを変更することで、より細かい粒度とパフォーマンスのチューニングが可能です。

プロファイルを適用するには

1. アカウントユニットを開きます。
2. プロファイルを選択します。

プロファイルを変更するには

1. 新しいプロフィールを作成します。
2. ユーザディレクトリのプロファイルの設定を新しいプロファイルにコピーします。
3. 値を変更します。

ユーザ情報の効率的な取得

ユーザディレクトリサーバは、さまざまな手段や関係によってグループやメンバを編成します。ユーザディレクトリの操作は、ユーザ、ユーザのグループ、およびテンプレート(テンプレートはグループエントリとして定義され、ユーザはそのメンバ) に対してCheck Pointによって実行されます。グループ/テンプレートやユーザを定義するモードは、ユーザ情報を取得する際のCheck Pointの一部の機能のパフォーマンスに大きく影響します。モードは3種類あります。

- メンバごとの "Member "属性、または"*Member*"ユーザ対グループのメンバシップ モードを定義。この場合、特定のグループの各メンバは"メンバ"属性を取得し、この属性の値はそのメンバのDNとなります。
- グループごとの "Memberof "属性、または"*MemberOf*"ユーザ間メンバシップモードの定義。この場合、グループごとに "Memberof "属性を取得し、この属性の値はグループエントリのDNです。これは「*MemberOf*」ユーザ対グループ メンバシップモードと呼ばれます。
- メンバおよびグループごとの "Memberof "属性、またはユーザとグループのメンバシップモード "*Both*"の定義。この場合、メンバとグループの両方に"Memberof "属性が与えられます。

最も効果的なモードは「MemberOf」と「Both」モードで、ユーザのグループメンバシップ情報がユーザ自身から得られるため、追加のユーザディレクトリクエリが不要になります。

User-to-Groupメンバシップモードの設定

`objects_5_0.C`ファイル内の各ユーザディレクトリサーバのプロファイルオブジェクトに、user-to-groupメンバシップモードを設定します。

- user-to-group、template-to-groupメンバシップモードを指定するには、`GroupMembership`属性を"`Member`"、"`MemberOf`"、"`Both`"のいずれかに適切に設定します。
- user-to-templateメンバシップモードを指定するには、`TemplateMembership`属性を"`Member`"、"`MemberOf`"のいずれかに適切に設定します。

データベースを正常に変換したら、`objects_5_0.C`ファイルのユーザディレクトリサーバプロファイルを適切なメンバシップ設定にし、Security Management Serverを起動します。

新しい設定を有効にするために、すべてのセキュリティゲートウェイにポリシー/ユーザデータベースをインストールします。

プロフィール属性

UserLoginAttr

一意のユーザ名ユーザディレクトリ属性(uid) 。

また、ユーザ名でユーザを取得する場合、この属性がクエリに使用されます。

デフォルト	その他
■ uid (ほとんどのサーバ) ■ SamAccountName (Microsoft_AD)	1つの値が可

ユーザパスワード属性

このユーザパスワードは、ユーザディレクトリ属性です。

デフォルト	その他
■ userPassword (ほとんどのサーバ) ■ unicodePwd (Microsoft_AD)	1つの値が可

テンプレートオブジェクトクラス

Check Pointユーザディレクトリテンプレートのオブジェクトクラス。

他のオブジェクトクラスでデフォルト値を変更する場合は、そのオブジェクトクラスのスキーマ定義を`fw1template`の関連属性で拡張してください。

デフォルト	その他
fw1template	複数値可

ExpirationDateAttr

アカウントの有効期限は、ユーザディレクトリ属性です。

この属性は、Check Pointの拡張属性、または既存の属性の場合があります。

デフォルト	その他
■ fw1expiration-date (ほとんどのサーバ) ■ accountExpires (Microsoft_AD)	1つの値が可

ExpirationDateFormat

有効期限の形式。

このフォーマットは、`ExpirationDateAttr`で定義された値に適用されます。

デフォルト	その他
CPのフォーマットはyyyymmdd	1つの値が可

PsswdDateFormat

パスワード更新日のフォーマットは、ユーザディレクトリ属性です。

定義された値に適用されます：`PsswdDateAttr`.

デフォルト	その他
■ CP(ほとんどのサーバ) のフォーマットは yyyymmdd ■ MS (Microsoft_AD)	1つの値が可

PsswdDateAttr

パスワードの最終更新日は、ユーザディレクトリの属性です。

デフォルト	その他
■ fw1pwdLastMod (ほとんどのサーバ) ■ pwdLastSet (Microsoft_AD)	1つの値が可

BadPwdCountAttr

パスワード認証の不正回数を保存し、読み取るためのユーザディレクトリの属性。

デフォルト	その他
fw1BadPwdCount	1つの値が可

ClientSideCrypt

0の場合、送信パスワードは暗号化されません。

1の場合、送信パスワードはDefaultCryptAlgorithmで指定されたアルゴリズムで暗号化されます。

デフォルト	その他
■ ほとんどのサーバは0 ■ Netscape_DSは1 暗号化パスワードを使用しない場合は、SSLを推奨します。	1つの値が可

DefaultCryptAlgorith

ユーザディレクトリサーバを新しいパスワードで更新する前に、パスワードを暗号化するために使用されるアルゴリズム。

デフォルト	その他
■ Plain (ほとんどのサーバ) ■ Crypt (Netscape_DS) ■ SHAI1	1つの値が可

CryptedPasswordPrefix

変更されたパスワードでユーザディレクトリサーバを更新する際に、暗号化されたパスワードのプレフィックスを付けるテキスト。

デフォルト	その他
{Crypt} (Netscape_DS)	1つの値が可

PhoneNumberAttr

ユーザの電話番号を保存し、読み取るためのユーザディレクトリ属性。

デフォルト	その他
internationalisednumber	1つの値が可

AttributesTranslationMap

異なるサーバタイプの特性に関連する問題を解決するための汎用属性変換マップ。

例えば、X.500サーバでは、属性名に"-"文字を使用できません。

"-"を含むCheck Point属性を有効にするには、変換エントリ: ("`fw1-expiration =fw1expiration`"など) を指定します。

デフォルト	その他
なし	複数値可

ListOfAttrsToAvoid

ここに記載されたすべての属性名は、読み取り/書き込み操作に含まれるデフォルトの属性リストから削除されます。

これは、これらの属性がユーザディレクトリサーバのスキーマでサポートされておらず、操作全体が失敗する可能性がある場合に、最も有効な方法です。

これは、ユーザディレクトリサーバのスキーマがCheck Pointのスキーマ拡張機能で拡張されていない場合に特に当てはまります。

デフォルト	その他
デフォルトでは値はありません。 ユーザディレクトリサーバがCheck Pointのスキーマによって拡張されていない場合。 新しいCheck Pointスキーマ属性をすべてリストするのが最善策です。	複数値可

BranchObjectClass

この属性は、SmartConsoleでアカウントユニットを開いた後、オブジェクトツリーの分岐を表示する際に、どのタイプのオブジェクト(objectclass) を照会するかを定義します。

デフォルト	その他
■ 組織 OrganizationalUnitドメイン(ほとんどのサーバ) ■ コンテナ (Microsoft_ADは別途)	複数値可

BranchOCOperator

"One"を設定すると、"OR "クエリが送信され、条件に一致するすべてのオブジェクトがブランチとして表示されます。

"All"を設定すると、"AND"のクエリが送信され、すべてのタイプのオブジェクトのみが表示されます。

デフォルト	その他
One	1つの値が可

OrganizationObjectClass

この属性は、どのオブジェクトが組織オブジェクトアイコンで表示されるべきかを定義します。

ここで指定された新しいオブジェクトタイプは、BranchObjectClassにも含まれる必要があります。

デフォルト	その他
組織	複数値可

OrgUnitObjectClass

この属性は、どのオブジェクトが組織オブジェクトアイコンで表示されるべきかを定義します。

ここで指定された新しいオブジェクトタイプは、BranchObjectClassにも含まれる必要があります。

デフォルト	その他
■ organizationalUnit (ほとんどのサーバ) ■ コンテナ(Microsoft_ADに追加)	複数値可

DomainObjectClass

この属性は、ドメインオブジェクトアイコンで表示されるべきオブジェクトを定義します。

ここで指定された新しいオブジェクトタイプは、BranchObjectClassにも含まれる必要があります。

デフォルト	その他
ドメイン	複数値可

UserObjectClass

この属性は、ユーザオブジェクトとして読み取るべきオブジェクトを定義します。

ここで指定したオブジェクトタイプのツリーに、ユーザアイコンが表示されます。

デフォルト	その他
■ User (Microsoft_AD) ■ Person OrganizationalPerson InertOrgPerson FW1 Person (ほとんどのサーバ)	複数値可

UserOCOperator

"One"を設定すると、"OR "クエリが送信され、いずれかのタイプにマッチするすべてのオブジェクトが、ユーザとして表示されます。

"All"を設定すると、"AND"のクエリが送信され、すべてのタイプのオブジェクトのみが表示されます。

デフォルト	その他
One	1つの値が可

GroupObjectClass

この属性は、グループとして読み取るべきオブジェクトを定義します。

ここで指定したタイプのオブジェクトには、ツリー上にグループアイコンが表示されます。

デフォルト	その他
■ Groupofnames ■ Groupofuniquenames (ほとんどのサーバ) ■ グループ ■ Groupofnames (Microsoft_AD)	複数値可

GroupOCOperator

"One"を設定すると、"OR "クエリが送信され、いずれかのタイプにマッチするすべてのオブジェクトが、ユーザとして表示されます。

"All"を設定すると、"AND"のクエリが送信され、すべてのタイプのオブジェクトのみが表示されます。

デフォルト	その他
One	1つの値が可

GroupMembership

グループメンバシップを読み取る際の、グループとそのメンバ(ユーザまたはテンプレートオブジェクト) の関係モードを定義します。

デフォルト	その他
■ メンバモードは、グループオブジェクトのメンバDNを定義(ほとんどのサーバ) ■ MemberOfモードでは、メンバオブジェクトのグループDNを定義(Microsoft_AD) ■ モードは、Groupオブジェクトにメンバ DNを、Memberオブジェクトにグループ DNを定義します。	1つの値が可

UserMembershipAttr

ユーザまたはテンプレートオブジェクトからグループメンバシップを読み取る際に使用するユーザディレクトリ属性を定義します。GroupMembershipモードが 'MemberOf' または 'Both' の場合、ユーザ/テンプレートオブジェクトのスキーマを拡張して、この属性を使用する必要がある可能性があります。

デフォルト	その他
MemberOf	1つの値が可

TemplateMembership

ユーザテンプレートメンバシップ情報を読み込む際の、ユーザからテンプレートメンバシップへのモードを定義します。

デフォルト	その他
■ メンバモードは、グループオブジェクトのメンバDNを定義(ほとんどのサーバ) ■ MemberOfモードでは、メンバオブジェクトのグループDNを定義(Microsoft_AD)	1つの値が可

TemplateMembershipAttr

TemplateMembershipモードがMemberである場合に、テンプレートオブジェクトからユーザDNとしてユーザメンバを読み取る際に使用する属性を定義します。

デフォルト	その他
member	複数値可

UserTemplateMembershipAttr

TemplateMembershipモードがMemberOfの場合に、ユーザオブジェクトからユーザに関連するテンプレートDNを読み取る際に使用する属性を定義します。

デフォルト	その他
member	複数値可

OrganizationRDN

この値は、SmartConsoleで新しい組織単位(OU)を作成するときに、相対識別名(RDN)の属性名として使用されます。

デフォルト	その他
o	1つの値が可

OrgUnitRDN

この値は、SmartConsoleで新しい組織単位(OU)を作成するときに、相対識別名(RDN)の属性名として使用されます。

デフォルト	その他
ou	1つの値が可

UserRDN

この値は、SmartConsoleで新しいユーザオブジェクトを作成する際に、相対識別名(RDN)の属性名として使用されます。

デフォルト	その他
cn	1つの値が可

GroupRDN

この値は、SmartConsoleで新しいグループオブジェクトを作成する際に、RDNの属性名として使用されます。

デフォルト	その他
cn	1つの値が可

DomainRDN

この値は、SmartConsoleで新しいドメインオブジェクトを作成するときに、RDNの属性名として使用されます。

デフォルト	その他
dc	1つの値が可

AutomaticAttrs

このフィールドは、SmartConsoleでオブジェクトを作成するときに関連します。

このフィールドのフォーマットは`Objectclass:name:value`です。したがって、作成されたオブジェクトが`ObjectClass`タイプである場合、作成されたオブジェクトに名前 '`name`' と値 '`value`' を持つ追加属性が含まれます。

デフォルト	その他
user:userAccountControl:66048 Microsoft_ADの場合 これは、ユーザオブジェクトの作成時に、userAccountControl (値66048) という追加属性が自動的に含まれることを意味します。	複数値可

GroupObjectClass

このフィールドは、SmartConsoleでグループを修正するときに使用します。

このフィールドのフォーマットは**ObjectClass:memberattr**で、各グループオブジェクトクラスにグループメンバシップの属性がマッピングされていることを意味します。

このユーザディレクトリサーバのプロファイルに可能なすべてのマッピングをここにリストアップします。

グループが変更された場合、グループのオブジェクトクラスに基づいて、正しいグループメンバシップマッピングが使用されます。

デフォルト	その他
■ groupOfNames:member ■ groupOfUniqueNames:uniqueMember (他のすべてのサーバ)	複数値可

OrgUnitObjectClass

OrganizationalUnitオブジェクトを作成/変更する際に使用するObjectClassを決定します。

これらの値は、読み取りの対応値と異なる場合があります。

デフォルト	その他
OrganizationalUnit	複数値可

OrganizationObjectClass

これは、組織オブジェクトを作成および/または変更するときに使用するObjectClassを決定します。

これらの値は、読み取りの対応値と異なる場合があります。

デフォルト	その他
組織	複数値可

UserObjectClass

これは、ユーザオブジェクトの作成時や変更時に使用するObjectClassを決定します。

これらの値は、読み取りの対応値と異なる場合があります。

デフォルト	その他
■ User (Microsoft_AD) ■ person ■ organizationalPerson ■ inetOrgPerson ■ fw1Person ■ (他のすべてのサーバ)	複数値可

DomainObjectClass

ドメインコンテキストオブジェクトを作成または変更する際に使用するObjectClassを決定します。

これらの値は、読み取りの対応値と異なる場合があります。

デフォルト	その他
ドメイン	複数値可

ユーザディレクトリサーバでのユーザ管 理

ユーザディレクトリサーバでのユーザ管 理

SmartConsoleでは、アカウント ユニット 内 のユーザとユーザグループは、LDAPサーバと同じツリー構造 で表 示 されます。

- ユーザディレクトリのユーザを確 認 には、**Users and Administrators**を開きます。**LDAP Groups**フォルダには、サーバの構 造 とアカウント があります。
- ユーザディレクトリのテンプレート は変 更 できます。このテンプレート に関 連 するユーザは、すぐに変 更 内 容 を取 得 します。SmartConsoleでユーザ定 義 を手 動 で変 更 した場 合 、変 更 内 容 はサーバ上 で即 座 に反 映 されます。

複 数 のサーバへのユーザの分 散

組 織 のユーザは、複 数 のLDAPサーバに分 散 できます。LDAPサーバは、それぞれ別 のAccount Unitで表 す必 要 があります。

LDAP情 報 の管 理

ユーザディレクトリでは、SmartDashboardを使 って、LDAPサーバに保 存 されているユーザやOU (Organizational Units) の情 報 を管 理 できます。

SmartDashboardからLDAP情 報 を管 理 するには

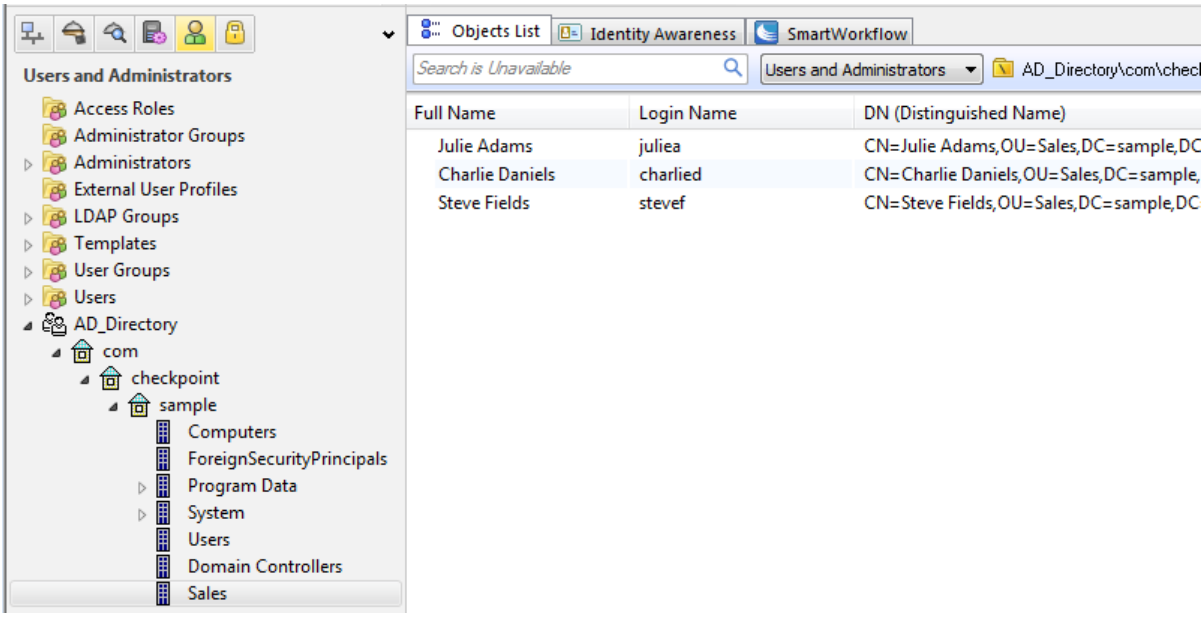
1. SmartConsoleで、**Manage & Settings > Blades**にアクセスします。
2. **Configure in SmartDashboard**をクリックします。

   SmartDashboardが開 きます。
3. オブジェクト ツリーから、**Servers and OPSEC**を選 択 します。
4. アカウント ユニット をダブルクリックします。

   LDAPドメインオブジェクト が開 きます。
5. LDAPブランチをダブルクリックします。

   Security Management ServerがLDAPサーバに照 会 し、SmartDashboardでLDAPオブジェクト が表 示 されます。
6. **Objects List**ペインを展 開 します。

   例 :



7. LDAPオブジェクトをダブルクリックします。

   Objects Listペインには、ユーザ情報が表示されます。

8. ユーザを右クリックし、**Edit**を選択します。

   LDAP User Propertiesウィンドウが開きます。

9. ユーザ情報と設定を編集します。クリック**OK**。

ユーザディレクトリのLDAPグループ

ユーザディレクトリのLDAPグループを作成します。これらのグループは、ユーザをタイプ別に分類し、ポリシールールで使用することができます。ユーザをグループに追加したり、動的なフィルタを作成したりすることができます。

ユーザディレクトリ用のLDAPグループを作成するには

1. SmartConsoleで、**Object Categories > New > More > Users > LDAP group**を開きます。
2. 開いた**New LDAP Group**ウィンドウで、ユーザディレクトリグループの**Account Unit**を選択します。
3. **Group's Scope**の定義 - いずれかを選択します。
   - **All Account-Unit's Users**- グループ内の全ユーザ
   - **Only Sub Tree**- 指定されたブランチのユーザ
   - **Only Group in branch**- 指定されたDNプレフィックスを持つブランチ内のユーザ
4. 高度な技術を適用する**LDAP filter:**

a. **Apply filter for dynamic group**をクリックします。

b. フィルタ条件を入力します。

5. クリック**OK**。

例:

- 組織内のマネージャーのユーザオブジェクトがオブジェクトクラス "myOrgManager "を持っている場合、フィルタを使用してマネージャーグループを定義します:**objectclass=myOrgManagers**
- 組織内のユーザがus.org.comで終わるEメールアドレスを持っている場合、フィルタを使用してUSグループを定義することができます:**mail=*us.org.com**

User Directoryサーバからの情報の取得

セキュリティゲートウェイが認証のためにユーザ情報を必要とするとき、このプロセスが行われます。

1. セキュリティゲートウェイは*内部管理データベース*でユーザを検索します。
2. 指定されたユーザが*内部管理*データベースに定義されていない場合、セキュリティゲートウェイは、アカウントユニットに定義されている*LDAPサーバ*に最優先で問い合わせします。
3. 最も高い優先順位を持つLDAPサーバへのクエリ失敗した場合(接続が切れたなど)、セキュリティゲートウェイは次に高い優先順位を持つサーバにクエリを行います。

   アカウントユニットが複数ある場合は、アカウントユニットを同時に照会します。クエリの結果は、条件を満たした最初のアカウントユニット、または条件を満たしたすべてのアカウントユニットから取得されます。
4. すべてのLDAPサーバに対するクエリが失敗した場合、セキュリティゲートウェイは一般的な外部ユーザプロファイルとユーザを照合します。

User Directoryのクエリの実行

クエリを使用して、User Directoryのユーザまたはグループデータを取得します。最高のパフォーマンスを得るには、接続が開いているときにアカウントユニットにクエリを実行します。一部の接続は、ユーザが特定の操作を許可されたグループに属していることを確認するために、セキュリティゲートウェイによって開かれたままになっています。

ユーザディレクトリに問い合わせる

1. SmartConsoleで、**Manage & Settings** >**Blades**と進みます。
2. **Configure in SmartDashboard**をクリックします。

   SmartDashboardが開きます。
3. **Objects Tree**で、**Users**をクリックします。
4. **Account Unit**をダブルクリックすると、LDAPサーバへの接続が開始されます。
5. **Account Unit**を右クリックし、**Query Users/Group**を選択します。

   LDAP Query Searchウィンドウが開きます。

   Advancedをクリックすると、ユーザ、グループ、テンプレートなど、指定したオブジェクトの種類を選択できます。
6. クエリを定義します。
7. さらに条件を追加するには、値を選択または入力し、**Add**をクリックします。

クエリの条件:

- **属性** - ドロップダウンリストからユーザの属性を選択するか、属性を入力します。
- **演算子** - ドロップダウンリストから演算子を選択します。

- **値** - エントリの属性と比較するための値を入力します。実際のユーザ属性と同じタイプとフォーマットを使用します。例えば、**属性**がfw1expiration-dateの場合、**値**は**yyyymmdd**構文でなければなりません。
- **フリーフォーム** - クエリ式を入力します。User Directory(LDAP) のクエリ式の構文については、RFC 1558を参照してください。
- **追加** - クエリに条件を追加します(**Search Method**の右側のテキストボックス) 。

クエリの例

次のクエリを作成した場合 :

- Attributes=mail
- Contains
- Value=Andy

サーバはこのフィルタでUser Directoryにクエリを行います。

```
filter:(&(|(objectclass=fw1person)(objectclass=person)
(objectclass=organizationalPerson)(objectclass=inetOrgPerson))
(|(cn=Brad)(mail=*Andy*)))
```

複数のLDAPサーバへのクエリ

Security Management Serverとセキュリティゲートウェイは、複数のLDAPサーバと同時に動作することができます。例えば、Security Gatewayがユーザ情報を見つける必要があり、指定されたユーザがどこで定義されているかがわからない場合、システム内のすべてのLDAPサーバに問い合わせます。(証明書を扱う場合、セキュリティゲートウェイはユーザDNを見ることでユーザの場所を見つけることができることがある)。

アカウント ユニット

アカウント ユニット は、1つまたは複 数 のLDAPサーバ上 のユーザ情 報 のブランチを表 します。アカウント ユニット は、LDAPサーバとSecurity Management ServerおよびSecurity Gatewayの間 のインタフェースです。

アカウント ユニット は、1つまたは複 数 のLDAPサーバを表 す数 を持 つことができます。ユーザは、1つのアカウント ユニット のブランチ間 、または異 なるアカウント ユニット 間 で分 割 されます。

注 - Identity Awareness and Mobile Access Software Bladeを有 効 にすると、SmartConsoleに初 期 設 定 ウィザード が表 示 されます。このウィザード の**Active Directory Integration**ウィンド ウでは、新 しいADアカウント ユニット を作 成 することができます。ウィザードを完 了 すると、SmartConsoleはADオブジェクト とアカウント ユニット を作 成 します。

LDAPアカウント 単 位 での作 業

SmartConsoleの**LDAP Account Unit Properties**ウィンド ウを使 用 して、既 存 のアカウント ユニット を新 規 作 成 または編 集 したり、手 動 で新 規 作 成 したりすることができます。

既 存 のLDAPアカウント ユニット を作 成 または編 集 するには

1. - **作 成** : **Objects**タブで、**New > More > User/Identity > LDAP Account unit**をクリックします。
   - **編 集** : SmartConsoleで、**Object Explorer** (**CTRL+E**キーを押 す) > **Users/Identities** > **LDAP Account Units** > LDAP Account Unitを右 クリックし、**Edit**を選 択 します。

   LDAP Account Unit Propertiesウィンド ウが開 きます。
2. これらのタブの設 定 を編 集 します。

■ **一般**

Security Management Serverでアカウントユニットをどう使用するかを設定します。

これらは、**General**タブの設定フィールドです。

- **Name**- アカウントユニット名
- **Comment**- 任意コメント
- **Color**- アカウントユニットに関連するオプションカラー
- **Profile**- LDAPベンダー
- **Domain**- 同じユーザ名が複数のアカウントユニットで使用されている場合、Active Directoryサーバのドメイン(この値はADクエリおよびSSOにも必要)
- **Prefix**- 同じユーザ名が複数のアカウントユニットで使用される場合の、非Active Directoryサーバのプレフィックス
- **Account Unit usage**- 該当するオプションを選択します:
  - **CRL retrieval**- Security Management Serverは、CAが失効したライセンスに関する情報をセキュリティゲートウェイに送信する方法を管理します。
  - **User Management**- Security Management Serverは、このLDAPサーバからのユーザ情報を使用します(Security Management Serverでユーザディレクトリが有効になっている必要がある) 。

    注 - LDAP SSO(シングルサインオン) は、**User Management**を使用するAccount Unitオブジェクトに対してのみサポートされます。
  - **Active Directory Query**- このActive Directoryサーバは、Identity Awarenessソースとして使用されます。

    注 - このオプションは、**Profile**が**Microsoft_AD**に設定されている場合のみ利用可能です。
- **Enable Unicode support**- 英語以外の言語によるLDAPユーザ情報のエンコーディング
- **Active Directory SSO configuration**- Active DirectoryのKerberos SSOをクリックして設定 - **Domain Name**、**Account Name**、**Password**、**Ticket encryption method**

■ **サーバ**

このアカウントユニットが使用するLDAPサーバを管理します。LDAPサーバのオブジェクトを追加、編集、削除することができます。

アカウントユニットにLDAPサーバを設定するには

a. 新しいサーバを追加するには、**Add**をクリックします。既存のものを編集するには、テーブルから選択して**Edit**をクリックします。

LDAP Server Propertiesウィンドウが開きます。

b. **Host**ドロップダウンメニューから、サーバオブジェクトを選択します。

必要に応じて、新しいSmartConsoleサーバオブジェクトを作成します。

i. クリック**New**。

ii. **New Host**ウィンドウが開いたら、LDAPサーバの設定を入力します。

iii. クリック**OK**。

c. ログイン認証情報と**Default priority**を入力します。

注 - LDAPアカウントユニットを作成してグループクエリを送信する場合、特別な権限は必要ありません。
Active Directoryクエリを送信するためにLDAPアカウントユニットを作成する場合、sk93938で提供されている権限が必要です。

d. Check Point Gatewayのアクセス権を選択します。

- **Read data from this server**
- **Write data to this server**

e. LDAP接続は、信頼する認証局(CA)から提供されるクライアント証明書を使用して認証できます。**Encryption**タブで、オプションのSSL暗号化設定を行います。

- **Use Encryption (SSL)**を使用すると、SSLを使用してLDAP接続を暗号化できます。該当する**Encryption port**番号を入力していることを確認してください。
- サーバ名、CA名、CAフィンガープリントを取得するには、**Fetch**をクリックします。
- **CRL check**を選択し、サーバ証明書が失効していないことを確認します。
- 証明書を使用するには、LDAPサーバがSSL**強力**暗号化で構成されている必要があります。

f. クリック**OK**。

アカウントユニットからLDAPサーバを削除するには

a. テーブルからサーバを選択します。

b. クリック**Remove**。

設定されているすべてのサーバが同じログイン情報を使用している場合は、すべてを同時に変更することができます。

すべてのサーバのログイン認証情報を同時に設定するには

a. **Update Account Credentials**をクリックします。

Update Account to All Serversウィンドウが開きます。

b. ログイン認証情報を入力します。

c. クリック**OK**。

■ **オブジェクト管理**

Security Management Serverが問い合わせるLDAPサーバと、使用するブランチを設定します。

注 - Security Management Serverと管理ディレクトリを保持するLDAPサーバの間にLDAP接続があることを確認してください。

LDAPクエリパラメータを設定するには

a. **Manage objects on**ドロップダウンメニューから、LDAPサーバオブジェクトを選択します。

b. **Fetch branches**をクリックします。

Security Management Serverは、LDAPブランチに問い合わせを行い、表示します。

c. **Branches in use**を設定します:

- ブランチを追加するには、**Add**をクリックし、開いたLDAP Branch Definitionウィンドウで、新しい**Branch Path**
- ブランチを編集するには、**Edit**をクリックして開いたLDAP Branch Definitionウィンドウで次を変更 : **Branch Path**
- ブランチを削除するには、ブランチを選択して**Delete**

d. 必要に応じて、**Prompt for password when opening this Account Unit**を選択します(オプション) 。

e. LDAPデータベースに保存される**Return entries**の数を設定します(デフォルトは 500) 。

- **認証**

  アカウントユニットの認証スキームを設定します。これらはAuthenticationタブの設定フィールドです。

  - **Use common group path for queries**- すべてのLDAPグループオブジェクトに1つのパスを使用するよう選択(グループオブジェクトに必要なクエリは1つだけ)
  - **Allowed authentication schemes**- このアカウントユニットでユーザを認証するために許可される1つ以上の認証スキームを選択 - **Check Point Password**、**SecurID**、**RADIUS**、**OS Password**、または**TACACS**
  - ユーザのデフォルト値 - 新しいLDAPユーザのデフォルト設定:
    - **User template**- 作成したテンプレート
    - **Default authentication scheme**- **Allowed authentication schemes**セクションで選択した認証スキームの1つ
  - **Limit login failures**(オプション):
    - **Lock user's account after**- **login failures**の後アカウントはロックされます
    - **Unlock user's account after-seconds**の後ロックされたアカウントはロック解除されます
  - **IKE pre-shared secret encryption key**- このアカウントユニットのIKEユーザ用の事前共有秘密鍵

3. クリック**OK**。
4. アクセスコントロールポリシーをインストールします。

LDAPクエリパラメータの設定

1. **Manage objects on**ドロップダウンメニューから、LDAPサーバオブジェクトを選択します。
2. **Fetch branches**をクリックします。

   Security Management Serverは、LDAPブランチに問い合わせを行い、表示します。
3. **Branches in use**を設定します:
   - ブランチを追加するには、**Add**をクリックし、開いたLDAP Branch Definitionウィンドウで、新しい**Branch Path**
   - ブランチを編集するには、**Edit**をクリックします。**Branch Path**
   - ブランチを削除するには、ブランチを選択して:**Delete**
4. 必要に応じて、**Prompt for password when opening this Account Unit**を選択します(オプ

ション) 。

5. LDAPデータベースに保存されるReturn entriesの数を設定します(デフォルトは 500) 。

LDAPサーバの変更

1. LDAPアカウント ユニット のプロパティ > サーバタブで、サーバをダブルクリックします。

   LDAP Server Propertiesウィンドウが表示されます。

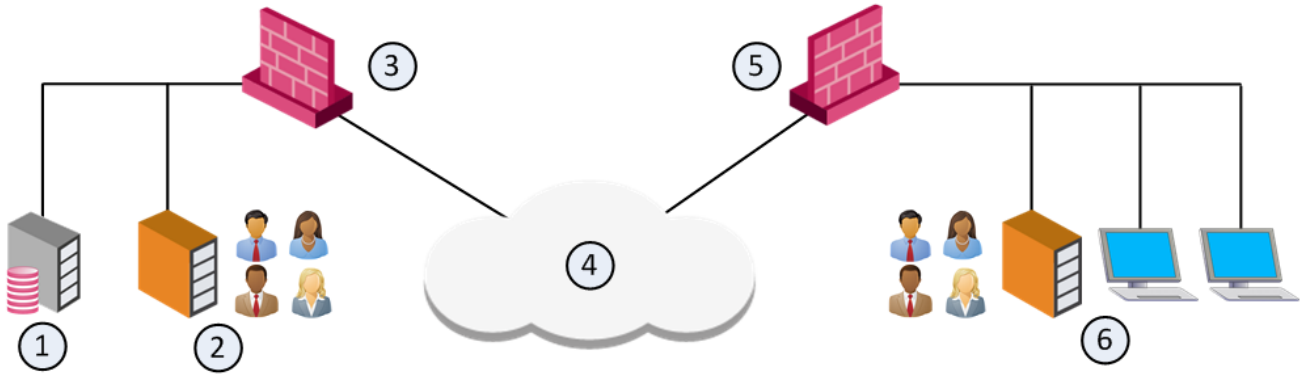
2. Generalタブで以下を変更します。
   - LDAPサーバのポート番号
   - ログインDN
   - パスワード
   - LDAPサーバの優先順位(複数サーバがある場合)
   - LDAPサーバのセキュリティゲート ウェイの権限
3. Encryptionタブでは、Security Management Server / Security GatewaysとLDAPサーバ間の暗号化設定を変更することができます。

   接続が暗号化されている場合は、暗号化ポートと暗号化強度の設定を入力します。

   注 - ユーザディレクトリ接続は、認証局(CA)からのクライアント証明書によって認証できます。証明書を使用するには、LDAPサーバにSSL強力認証が設定されている必要があります。参照: *証明書での認証 (216ページ)*。

アカウント ユニットとハイアベイラビリティ

ハイアベイラビリティのためのユーザディレクトリのレプリケーションでは、1つのアカウント ユニットが複製されたすべてのユーザディレクトリサーバを表します。例えば、1つのアカウント ユニットに2つのUser Directoryサーバのレプリケーションを定義し、2つのセキュリティゲート ウェイで同じアカウント ユニットを使用することができます。



項目	説明
1	**Security Management Server**。User Directoryのユーザデータを管 理します。2つのサーバが定 義されるAccount Unitオブジェクト を持ちます。
2	**User Directory server**レプリケーション。
3	**セキュリティゲート ウェイ**。ユーザデータのクエリを行い、最も近いUser Directoryサーバのレプリケーションから CRLを取 得します(2) 。
4	インターネット
5	**セキュリティゲート ウェイ**。ユーザデータのクエリを行い、最も近いUser Directoryサーバのレプリケーションから CRLを取 得します(6) 。
6	**User Directory server**レプリケーション。

ハイアベイラビリティ優 先 度 の設 定

複 数 のレプリケーションがある場 合 、アカウント ユニット で各 LDAPサーバの優 先 度 を定 義します。次に、セキュリティゲート ウェイのサーバリスト を定 義します。

Security Management Serverが接 続 するLDAPサーバを1つ選 択します。Security Management Serverは、1つのLDAPサーバのレプリケーションで動 作させることができます。他 の複 製 はすべてスタンバイのために同 期 する必 要 があります。

アカウント ユニット の優 先 順 位 を設 定 するには

1. **LDAP Account Unit Properties**ウィンドウを開きます。
2. **Servers**タブを開きます。
3. このアカウント ユニット のLDAPサーバを、希 望 する優 先 順 位 で追 加します。

証 明 書 での認 証

Security Management Serverとセキュリティゲート ウェイは、証 明 書 を使 用してLDAPサーバとの通 信を保 護 できます。証 明 書 を設 定しない場 合 、管 理 サーバ、セキュリティゲート ウェイ、およびLDAPサーバは、認 証なしで通 信します。

証 明 書 を使 用するようにユーザディレクトリを設 定 するには

1. Management Serverに接 続 しているSmartConsoleのウィンドウをすべて閉じます。
2. 証 明 書 による認 証を行う各 アカウント ユニット で、`ldap_use_cert_auth`属 性 を`true`に設 定します。

a. 接続: *Database Tool (GuiDBEdit Tool)*を管理サーバに接続します。

b. 左側のペインで、**Table > Managed Objects > servers**に移動します。

c. 右側のペインで、Account Unitオブジェクトを選択します。

d. 下のペインで、`ldap_use_cert_auth`属性を検索し、**true**に設定します。

e. 変更を保存して、データベースツール(GuiDBEdit Tool) を閉じます。

3. SmartConsoleで管理サーバに接続します。

4. CAオブジェクトを追加します。

a. オブジェクトエクスプローラー(F11) で、**New** > **More** > **Server** > **More** > **Trusted CA**をクリックします。

認証局のプロパティウィンドウが表示されます。

b. 認証局タイプで、**External Check Point CA**を選択します。

c. CAのその他のオプションを設定します。

5. 証明書ベースのユーザディレクトリ接続を必要とするすべての必要なネットワークオブジェクト(Security Management Server、Security Gateway、Policy Serverなど) の場合:

a. ネットワークオブジェクトプロパティの**IPSec VPN**ページで、**Repository of Certificates Available**リストから**Add**をクリックします。

注 - 管理専用サーバには、IPsec VPN ページはありません。管理専用サーバのユーザディレクトリは、証明書を使用してLDAPサーバに認証するように設定することはできません。

b. **Certificate Properties**ウィンドウで、定義済みのCAを選択します。

6. Security Management ServerとLDAP Server間の接続をテストします。

参照: *LDAP情報の管理 (204ページ)*。

外部LDAPサーバ上のユーザの設定

LDAP は、Check Point Quantum がサポートする外部アイデンティティ統合技術です。

LDAPはこれらの機能を提供します:

- セキュリティゲートウェイは、LDAP データを使用してユーザを認証・認可することができます。
- セキュリティゲートウェイは、証明書情報を使用する際にCRL を取得できます。

その他のアイデンティティ統合オプションには、以下のものがあります:Check Point Quantum管理の内部ユーザデータベース、Entra ID、および Check Point Infinity Identity。

Microsoft Active Directory

Microsoft Active Directoryの概要についてはActive Directory Domain Servicesを参照してください。

ブランチ`CN=Schema, CN=Configuration, DCROOT`には、すべてのスキーマ定義が含まれています。

Check Pointは、既存のActive Directoryオブジェクトを利用するだけでなく、新しいタイプを追加することもできます。ユーザについては、既存のユーザを「そのまま」使用するか、「User」の補助として`fw1person`で拡張することで、機能の粒度を揃えることが可能です。既存のActive Directoryの「グループ」タイプは、「そのまま」サポートされます。`fw1template`オブジェクトクラスを追加することで、ユーザディレクトリテンプレートを作成することができます。この情報は、`schema_microsoft_ad.ldif`ファイルを使ってディレクトリにダウンロードされます (*Active Directoryへの新しい属性の追加 (220ページ)*)。

パフォーマンス

特定のSoftware Bladesでは、Active Directoryグループに関連する情報はユーザオブジェクトに保存されます。したがって、ユーザオブジェクトをフェッチする際、グループをユーザに割り当てるために追加のクエリは必要ありません。ユーザとテンプレートについても同様です。場合によっては、セキュリティゲートウェイは追加のクエリを送信します。sk128212を参照してください。

管理

SmartDashboardでは、既存および新規オブジェクトの作成と管理が可能です。ただし、一部のActive Directoryフィールドは SmartDashboardで有効になりません。

実施

スキーマを拡張することなく、既存のActive Directoryオブジェクトを扱うことができます。これは、内部テンプレートオブジェクトを定義し、Active Directoryサーバで定義されたユーザディレクトリアカウントユニットを割り当てることで可能となります。

たとえば、Active Directoryのパスワードに基づくIKE+ハイブリッドですべてのユーザを有効にする場合、IKEのプロパティを有効にし、認証方法に「Check Pointパスワード」を指定したテンプレートを新規に作成します。

レジストリ設定の更新

Active Directoryのスキーマを変更するには、`Schema Update Allowed`という新しいレジストリDWORDキーを追加し、`HKLM\System\CurrentControlSet\Services\NTDS\Parameters`の下にゼロ以外の値を設定します。

制御の委任

デフォルトでは、システム管理者はスキーマを変更したり、ユーザーディレクトリプロトコルを介してディレクトリオブジェクトを管理することさえできないため、ディレクトリの制御を特定のユーザまたはグループに委譲することは重要です。

ディレクトリの制御を委譲するには

1. ドメインコントローラで、Active Directory**ユーザとコンピュータコントロール**コンソールを開きます。
2. 左側のペインに表示されているドメイン名を右クリックし、右クリックメニューから **[コントロールの委譲]**を選択します。

   Delegation of Control wizardウィンドウが表示されます。
3. ディレクトリを制御できるユーザリストにユーザまたはグループを追加します。
4. マシンを再起動します。

Active Directoryスキーマの拡張

SmartConsoleでActive Directoryのユーザを設定するために、Active Directoryスキーマでファイルを変更します。

Active Directoryスキーマを拡張するには

1. セキュリティゲートウェイからスキーマファイルのあるディレクトリ`$FWDIR/lib/ldap`に移動します。
2. Active Directoryサーバの**C:**ドライブに`schmea_microsoft_ad.ldif`をコピーします。
3. Active Directoryサーバから、テキストエディタでスキーマファイルを開きます。
4. 値`DOMAINNAME`を見つけ、LDIF形式のドメイン名で置き換えます。

   例えば、LDIF形式のドメイン`sample.checkpoint.com`
   ：`DC=sample,DC=checkpoint,DC=com`
5. `modify`セクションの最後にダッシュ文字(-) があることを確認してください。

これは、modifyセクションの例です。

```
dn: CN=User,CN-
Schema,CN=Configuration,DC=sample,DC=checkpoint,DC=com
changetype: modify
add: auxiliaryClass
auxiliaryClass: 1.3.114.7.3.2.0.2
-
```

6. 次を実行します:

```
ldifde -i -f c:/schema_microsoft_ad.ldif
```

Active Directoryへの新しい属性の追加

以下は、Microsoft Active Directoryに1つの属性を追加する方法を示すLDAP Data Interchange (LDIF)フォーマットの例です:

```
dn:CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
changetype: add
adminDisplayName: fw1auth-method
attributeID: 1.3.114.7.4.2.0.1
attributeSyntax: 2.5.5.4
cn: fw1auth-method
distinguishedName:
CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
instanceType: 4
isSingleValued: FALSE
LDAPDisplayName: fw1auth-method
name: fw1auth-method
objectCategory:
CN=Attribute-
Schema,CN=ConfigurationCN=Schema,CN=Configuration,DCROOT
ObjectClass: attributeSchema
oMSyntax: 20
rangeLower: 1
rangeUpper: 256
showInAdvancedViewOnly: TRUE
```

Check Pointのすべての属性を同じ方法で追加できます。

LDIF形式のすべての属性の定義は、$FWDIR/lib/ldapディレクトリにあるschema_ microsoft_ad.ldifファイルに含まれています。

ldapmodifyコマンドを実行する前に、schema_microsoft_ad.ldifを編集し、DCROOTのすべてのインスタンスを組織のドメインルートに置き換えます。例えば、ドメインがsupport.checkpoint.comの場合、DCROOTをdc=support,dc=checkpoint,dc=comに置き換えます。

ファイルを修正した後、`ldapmodify`コマンドを実行して、ファイルをディレクトリに読み込みます。例えば、`dc=support,dc=checkpoint,dc=com domain`のシステム管理者アカウントを使用する場合、コマンド構文は以下のようになります:

注 - UNIXゲートウェイでは、シェルスクリプトが利用できます。スクリプト:`$FWDIR/lib/ldap/update_schema_microsoft_ad`

```
ldapmodify -c -h support.checkpoint.com -D
cn=administrator,cn=users,dc=support,dc=checkpoint,dc=com" -w
SeCrEt -f $FWDIR/lib/ldap/schema_microsoft_ad.ldif
```

Active Directory上のLDAPアカウントユニットに対するユーザまたはサービスアカウントのパスワードの更新

セキュリティゲートウェイは、SmartConsoleのLDAPアカウントユニットに保存されたLDAPサーバのユーザ名とパスワードを使用して、LDAPサーバに認証されます。セキュリティゲートウェイからLDAPサーバへの接続を確立した後、セキュリティゲートウェイはこの接続を再利用して、再認証を受けることなく以降のLDAPクエリを送信します。

LDAPサーバのActive Directoryでパスワードを更新した場合、変更を適用するには以下の手順を実行する必要があります:

1. LDAPアカウントユニットの情報を更新します。
2. ポリシーのインストール

ゲートウェイの管理

ここでは、セキュリティゲートウェイの作成、更新、管理と、Check Pointプラットフォームと製品のSIC(Secure Internal Communication) 方式による相互認証の方法について説明します。

SIC (Secure Internal Communication)

Check Pointのプラットフォームや製品は、これらのSIC(Secure Internal Communication) 方式のいずれかによって互いに認証されます。

- 証明書。
- 安全なチャネルを構築するための標準規格に準拠したTLS。
- 暗号化。

SICは、セキュリティゲートウェイ、管理サーバ、およびその他のCheck Point製品間の信頼できる接続を構築します。セキュリティゲートウェイにポリシーをインストールし、セキュリティゲートウェイと管理サーバ間でログを送信するには、信頼(Trust) が必要です。

注 - SICエラーを確認するには、Security Management ServerおよびSecurity Gateway上の`$CPDIR/log/sic_info.elg`ファイルを調べます。

トラストの初期化

セキュリティゲートウェイとSecurity Management Serverでは、最初の信頼関係を構築するためにワンタイムパスワードを使用します。最初の信頼が確立された後の通信はセキュリティ証明書に基づいて行われます。

注 - セキュリティゲートウェイとSecurity Management Serverの信頼関係を初期化する前に、セキュリティゲートウェイとSecurity Management Serverの時計が同期していることを確認してください。これはSICが成功するために必要なことです。セキュリティゲートウェイとSecurity Management Serverの時間設定を行うには、**Gaia Portal** >**System Management** >**Time** にアクセスします。

トラストを初期化するには

1. SmartConsoleで、セキュリティゲートウェイのネットワークオブジェクトを開きます。
2. セキュリティゲートウェイの**General Properties**ページで、**Communication**をクリックします。
3. **Communication**ウィンドウに、セキュリティゲートウェイのインストール時に作成した**Activation Key**を入力します。
4. クリック**Initialize**。

   ICAが署名し、セキュリティゲートウェイに証明書を発行します。

トラスト状態は、**Initialized but not trusted**(初期化済みで信頼されていない)です。内部認証局(ICA)はセキュリティゲートウェイの証明書を発行しますが、まだ送信していません。

通信する2つのピアは、共有されたアクティベーションキーを使ってSSL上で認証します。証明書は安全にダウンロードされ、セキュリティゲートウェイに保存されます。アクティベーションキーが削除されます。

セキュリティゲートウェイは、同じICAで署名されたセキュリティ証明書を持つCheck Pointホストと通信することができます。

SICステータス

ICAが発行した証明書をセキュリティゲートウェイが受け取った後、Security Management Serverがこのセキュリティゲートウェイと安全に通信できるかどうかをSICステータスで表示します。

- **Communicating** - 安全な通信が確立されています。
- **Unknown** - セキュリティゲートウェイとSecurity Management Serverとの間に接続がありません。
- **Not Communicating** - Security Management Serverはセキュリティゲートウェイにコンタクトすることができますが、SICを確立することができません。メッセージには詳細が表示されます。

トラスト状態

トラスト状態が侵害された場合(キーの流出、証明書の紛失)、またはオブジェクトが変更された場合(ユーザの退職、オープンサーバがアプライアンスにアップグレード)、トラスト状態をリセットします。トラストをリセットすると、SICの証明書は失効します。

証明書失効リスト(CRL)は、失効した証明書のシリアル番号について更新されます。ICAは更新されたCRLに署名し、次のSIC接続時にすべてのセキュリティゲートウェイに発行します。2つのセキュリティゲートウェイが異なるCRLを持つ場合、認証を行うことができません。

1. SmartConsoleのゲートウェイ & サーバビューで、セキュリティゲートウェイオブジェクトをダブルクリックします。
2. クリック**Communication**。
3. 開いた**Trusted Communication**ウィンドウで、**Reset**をクリックします。
4. ポリシーをセキュリティゲートウェイにインストールします。

   これにより、更新されたCRLがすべてのセキュリティゲートウェイに配布されます。ルールベースがない(したがって、ポリシーをインストールできない)場合、セキュリティゲートウェイの信頼をリセットすることができます。

   重要 - SmartConsoleで新しい信頼関係を確立する前に、同じワンタイムアクティベーションパスワードがセキュリティゲートウェイに設定されていることを確認します。

SICのトラブルシューティング

SICの初期化に失敗した場合:

1. セキュリティゲートウェイとSecurity Management Serverの間に接続性があることを確認します。
2. Security Management Serverとセキュリティゲートウェイが同じSICアクティベーションキー(ワンタイムパスワード)を使用していることを確認します。
3. Security Management Serverがゲートウェイの背後にある場合、Security Management Serverとリモートのセキュリティゲートウェイ間の接続を許可するルールがあることを確認します。アンチスプーフィングの設定が正しいことを確認します。
4. セキュリティゲートウェイの`/etc/hosts`ファイルにSecurity Management Serverの名前とIPアドレスが記載されていることを確認します。

   Security Management Server のIP アドレスがローカルのセキュリティゲートウェイによって静的NATでマッピングされている場合、Security Management Serverのパブリック IP アドレスをリモートのセキュリティゲートウェイの`/etc/hosts`ファイルに追加します。IPアドレスがサーバのホスト名に解決されることを確認します。
5. OSの日付と時刻の設定が正しいかどうか確認します。Security Management Serverとリモートのセキュリティゲートウェイが異なるタイムゾーンに存在する場合、リモートのセキュリティゲートウェイは証明書が有効になるまで待たなければならないことがあります。
6. 再度SICの確立を試みます。

リモートユーザによるリソースへのアクセス、モバイルアクセス

Mobile Access Software Bladeがすでに有効になっているセキュリティゲートウェイに証明書をインストールする場合、ポリシーを再度インストールする必要があります。そうでなければ、リモートユーザはネットワークリソースに到達できません。

セキュリティゲートウェイに新しい信頼状態を確立するには

1. セキュリティゲートウェイのコマンドラインインタフェースを開きます。
2. 次を実行します:

   cpconfig
3. **Secure Internal Communication**の数字を入力し、Enterキーを押します。
4. 「**y**」を入力して確認します。
5. アクティベーションキーを入力して確認します。
6. 完了したら、**Exit**の番号を入力します。
7. Check Pointのプロセスが停止し、自動的に再起動するのを待ちます。

SmartConsoleで:

1. セキュリティゲートウェイの**General Properties**ウィンドウで、**Communication**をクリックします。
2. **Trusted Communication**ウィンドウに、セキュリティゲートウェイで入力したワンタイムパスワード(アクティベーションキー)を入力します。
3. クリック**Initialize**。
4. **Certificate State**フィールドに**Trust established**と表示されるのを待ちます。
5. クリック**OK**。

Check Point内部認証局 (ICA) について

ICA(Internal Certificate Authority) は、Security Management Serverを初めて設定する際に作成されます。ICAは、認証のための証明書を発行します。

- **Secure Internal Communication (SIC)** - Security Management Server間、およびセキュリティゲートウェイとSecurity Management Servers間の通信を認証します。
- **ゲートウェイ用VPN証明書** - VPNコミュニティのメンバ間で認証を行い、VPNトンネルを作成します。
- **ユーザ** - 認証と権限に基づいてユーザアクセスを認証する強力な方法。

ICAクライアント

ほとんどの場合、証明書はオブジェクト設定の一部として扱われます。ICAと証明書をより詳細に制御するには、これらのICAクライアントのいずれかを使用します。

- Check Point Configuration Tool - これは、`cpconfig` CLI ユーティリティです。オプションの1つはICAを作成し、Security Management Server用のSIC証明書を発行します。
- SmartConsole - セキュリティゲートウェイおよび管理者用のSIC証明書、VPN証明書、ユーザ証明書。
- *ICA管理ツール (641ページ)*- ユーザ用のVPN証明書と高度なICA操作。

SmartConsole **Logs & Events** >**New Tab** > **Open Audit Logs View**のICAの監査ログを参照してください。

SIC証明書の管理

SIC証明書を管理する:

- **Communication**タブをクリックします。
- *ICA管理ツール (641ページ)*。

証明書には、以下のような設定可能な属性があります。

属性	デフォルト	コメント
有効	5年	
キーサイズ	2048ビット	
KeyUsage	5	デジタル署名と鍵の暗号化
ExtendedKeyUsage	0 (KeyUsageなし)	VPN証明書のみ

キーサイズの値について詳しくは、RSA key lengthsを参照してください。

各Software Bladeのライセンス情報を表示するには

ステップ	手順
1	セキュリティゲートウェイまたはSecurity Management Serverを選択します。
2	下のSummaryタブで、オブジェクトのLicense Status (例:OK) をクリックします。 Device & License Informationウィンドウが開きます。各Software Bladeの基本的なオブジェクト情報およびLicense Status、ライセンスExpiration Date、重要なクォータ情報 (Additional Infoカラム) が表示されます。 **注:** ■ クォータ情報、クォータに依存するライセンスステータス、およびブレード情報メッセージは、R80以降でのみサポートされています。 ■ SKUのツールチップはプロダクト名です。

Software BladeのLicense Statusに指定できる値は次のとおりです。

ステータス	説明
Active	Software Bladeが有効で、ライセンスも有効です。
Available	Software Bladeは非アクティブで、ライセンスは有効です。
No License	Software Bladeは有効ですが、ライセンスが無効です。
Expired	Software Bladeは有効ですが、ライセンスが失効しています。
About to Expire	Software Bladeは有効ですが、ライセンスの有効期限は30日 (デフォルト) 以内 (評価ライセンスの場合は7日以内) です。
Quota Exceeded	Software Bladeはアクティブで、ライセンスも有効ですが、関連オブジェクト (Security Gateway、Virtual Systems、ファイルなどBladeによって異なる) のクォータを超過しています。

ステータス	説明
Quota Warning	Software Bladeはアクティブで、ライセンスも有効ですが、このブレードのオブジェクト数がライセンス枠の90%(デフォルト)以上です。
N/A	ライセンス情報は利用できません。

セキュリティゲートウェイの新規作成

セキュリティゲートウェイは、Security Management Serverで設定されたセキュリティポリシーを実施します。

セキュリティゲートウェイにセキュリティポリシーをインストールするには、SmartConsoleでSecurity Gatewayオブジェクトを設定します。

新しいセキュリティゲートウェイオブジェクトを定義するには

1. ナビゲーションツールバーから、ゲートウェイ & サーバを選択します。
2. **New**をクリックし、**Gateway**を選択します。

   Check Point Security Gateway Creationウィンドウが開きます。
3. **Classic Mode**をクリックします。

   Check Point Gatewayプロパティウィンドウが開き、**General Properties**画面が表示されます。
4. ホストの**Name**と**IPv4 Address**または**IPv6 Address**を入力します。
5. クリック**Communication**。

   Trusted Communicationウィンドウが開きます。
6. **Platform**を選択します。

   重要 - 必ず正しいアプライアンスモデルを選択してください。そうでない場合、ポリシーのインストールに失敗することがあります。
7. **Authentication**セクションで、**One-time password**を入力し、確認します。

   Small Office Applianceプラットフォームを選択した場合、**Initiate trusted communication automatically when the Gateway connects to the Security Management Server for the first time**が選択されていることを確認します。
8. クリック**Initialize**セキュリティゲートウェイとの信頼された通信を確立します。*SIC (Secure Internal Communication) (222ページ)*)。

信頼関係の確立に失敗した場合は、**OK**をクリックしてセキュリティゲートウェイの設定を続行します。

9. クリック**OK**。
10. **Get Topology Results**ウィンドウが開き、セキュリティゲートウェイで正常に設定されたインタフェースが表示されます。
11. クリック**Close**。
12. **Platform**セクションで、**Hardware**、**Version**、**OS**を選択します。

    サーバとセキュリティゲートウェイの間に信頼関係が確率されている場合は、**Get**をクリックしてセキュリティゲートウェイから情報を自動的に取得します。
13. セキュリティゲートウェイで有効にするSoftware Bladesを選択します。

    一部のSoftware Bladeでは、初回セットアップウィザードが表示されます。ウィザードは今すぐでもあとでも実行できます。セットアップウィザードの詳細については、関連する管理ガイドを参照してください。

注 - Security Gatewayオブジェクトに追加の情報フィールドを追加することはできません。

ゲートウェイトポロジの手動更新

ネットワークの変更に伴い、セキュリティゲートウェイのトポロジを更新する必要があります。

セキュリティゲートウェイのトポロジを更新するには

1. SmartConsoleで、**Gateways & Servers**をクリックします。
2. Security Gatewayオブジェクトを右クリックします。

   セキュリティゲートウェイのプロパティウィンドウが表示されます。
3. **Network Management**をクリックします。
4. **Get Interfaces**をクリックし、該当するオプションを選択します。
   - **Get Interfaces With Topology**

     既存のトポロジとアンチスプーフィングの設定を上書きするかどうかを確認する警告ウィンドウが表示されます。

     Yesをクリックします。

     注 - ブリッジインタフェースの一部である物理インタフェースは、常にトポロジが「Undefined」で表示されます。
     回避策：APIコマンド "get-interfaces"を使用します。
   - **Get Interfaces Without Topology**
5. **Get Topology Results**ウィンドウが開きます。
6. クリック**Accept**。
7. インタフェースに適用できるトポロジとアンチスプーフィングを設定します。
8. クリック**OK**。
9. アクセスコントロールポリシーをインストールします。

インタフェースの取得 API

Check Point API を使用して、Get Interfaces コマンドを実行できます。

Get Interfaces API:

- SmartConsoleと比較して、より多くのインタフェースをサポートします。
- SmartConsoleでサポートされていないインタフェース(IPアドレスを持たないブリッジおよびボンドインタフェース) をサポートします。
- セキュリティゲートウェイとClusterXL R80.20以降の内部ネットワークのデフォルトトポロジを、該当する場合は**Network defined by routes**に設定します(SmartConsoleでのデフォルトは**This network (Internal)**) 。
- 不要なBridgeやBondのサテライトインタフェースは取得しません。

Get Interfaces APIコマンドは、Gaiaオペレーティングシステム上で動作するセキュリティゲートウェイとClusterXLのみをサポートしています。

API Getインタフェースコマンドの使い方については*Check Point Management API Reference*。

セキュリティゲートウェイトポロジの動的な更新

この機能は、Security Gateway R77.20以降でのみサポートされています。一度選択すると、管理者がGet Interfacesをクリックしてポリシーをインストールしなくても、内部インタフェースの背後にあるIPアドレスの範囲が1秒ごとに自動的に計算されます(デフォルト値)。

ダイナミックトポロジの更新を設定するには

1. Gateway Properties > Network Managementを開きます。
2. インタフェースを選択してEditをクリックします。
3. Topologyセクションで、Modifyをクリックします。
4. Leads Toセクションで、Network defined by routesを選択します。
5. クリックOK。

このデフォルトの更新値は、SmartConsole > Preferencesで設定され、1秒に設定されています。ここで設定した値は、ドメイン内のすべてのゲートウェイの内部インタフェースに適用されます。

特定のインタフェースの更新値を設定する場合

1. Gateway Properties > Network Managementを開きます。
2. インタフェースを選択してActions > Settingsをクリックします。
3. Use custom update time (seconds)を選択し、該当する更新時刻を設定します。
4. クリックOK。

動的アンチスプーフィング

アンチスプーフィングが選択されている状態でGet interfacesをクリックすると、インタフェースのIPアドレスとネットマスク、およびインタフェースに割り当てられたルートに基づいて、セキュリティゲートウェイが有効なIPアドレスのリストを生成します。

アンチスプーフィングは、パケットのインタフェースの背後にあるネットワークに属さない送信元IPアドレスを持つパケットをドロップします。例えば、外部インタフェースから来る内部IPアドレスのパケットなどです。

Network defined by routesとともに、Perform Anti-Spoofing based on interface topologyオプションを選択すると、*Dynamic Anti-Spoofing* が適用されます。有効なIPアドレスの範囲は、管理者がクリック(Get Interfaces) やポリシーのインストールをしなくても、自動的に計算されます。

ライセンスの管 理

Security Management Serverで初期設定ウィザードを実行し、Security Management Serverがユーザセンターへ接続すると、自動的にライセンスが有効になります。ライセンスが有効になる前にSecurity Management Serverでインターネット接続が切断された場合、間隔をあけて再試行されます。

Check PointユーザセンターでSecurity Management ServerのManagement Software Bladeライセンスに変更を加えると、その変更は自動的にそのSecurity Management Serverと同期されます。

注

- 自動アクティベーションは、Check Pointのアプライアンスでのみサポートされています。
- 自動同期機能は、R80.30以降のすべてのサーバでサポートされています。

Security Management Serverがインターネットに接続されていない場合でも、ユーザセンターと環境が同期されるようにするには、インターネットに接続可能なCheck Pointのサーバをプロキシとして設定することをお勧めします。

サーバとゲートウェイのライセンス管理

R81から、SmartConsoleでライセンスの手動追加、削除ができるようになりました。

ライセンスの追加と削除

ステップ	手順
1	SmartConsoleの左側のナビゲーションパネルから、**Gateways & Servers**をクリックします。
2	上部ペインで、該当するManagement ServerまたはSecurity Gatewayのオブジェクトを選択します。
3	下のペインで、**Licenses**タブをクリックします。
4	ライセンスの追加/削除： ■ ライセンスファイルからライセンスを追加するには a. **Add**をクリックし、**License File**を選択します。 b. ライセンスファイルを参照します。 c. ライセンスファイルを選択します。 d. **Open**をクリックします。 ■ ライセンス文字列からライセンスを追加するには a. **Add**をクリックし、**License String**を選択します。 b. ライセンス文字列を貼り付けます。 c. クリック**OK**。 ■ ライセンスを削除するには a. 一番左のカラムのライセンスを選択します。 b. **Remove**をクリックします。

注 -**Licenses** タブでライセンスを追加または削除するには、管理者のプロファイルで **Run One Time Script** 権限が選択されている必要があります。この権限を割り当てるには、SmartConsole で**Manage & Settings** >**Permissions & Administrators** >**Permission Profiles** に進みます。該当する権限プロファイルを開き、**Gateways** >**Scripts** と進み、**Run One-Time Scripts**を選択します。
参照 : *管理者への権限プロファイルの割り当て (116ページ)*

これらのカラムには、ライセンス情報が表示されます。

カラム	説明
IP Address	このライセンスが生成されたIPアドレス。
Expiration Date	Check Pointのサポート契約が終了する日。
CK	ライセンスインスタンスの一意の証明書キー。
SKU	Check Point User CenterからのカタログID。

注 - SmartConsole R81以降では、Gaia Embedded OSを搭載したQuantum Sparkアプライアンスのライセンスの表示はサポートされていません("ゲートウェイ & サーバ" ビューで、セキュリティゲートウェイオブジェクトを選択 > 下部のペインで "Licenses "タブをクリック) 。
回避策 : SmartUpdateを使用してライセンスを表示します。

重要 - CloudGuard IaaSセキュリティゲートウェイにライセンスを配布するには: *R82 CloudGuard Controller Administration Guide*。

SmartConsoleでのライセンスの表 示

ライセンス情 報を見 るには

ステップ	手 順
1	左 側 のナビゲーションパネルでGateways & Serversをクリックします。
2	Columnsドロップダウンリスト から、Licensesを選 択します。

次 のようなカラムを見 ることができます。

カラム	説 明
License Status	Software Bladeのライセンスの一 般 的 な状 態 です。 ■ OK- ブレードライセンスはすべて有 効 です。 ■ Not Activated- ブレードライセンスはインストールされていません。これは、SICがSecurity Management Serverとの間 で確 立 されてから最 初 の15日 間 だけ可 能 です。最 初 の15日 間 を過 ぎると、ライセンスがない場 合 、ブレードのエラーメッセージが表 示 されます。 ■ Error with <number> blade(s)- 指 定 された数 のブレードライセンスがインストールされていないか、有 効 ではありません。 ■ Warning with <number> blade(s)- 指 定 された数 のブレードライセンスに警 告 があります。 ■ N/A- 入 手 可 能 な情 報 はありません。
CK	ライセンスインスタンスの一 意 の証 明 書 キー。
SKU	Check Point User CenterからのカタログID。
Account ID	ユーザのアカウントID。
Support Level	Check Pointのサポートレベル。
Support Expiration	Check Pointのサポート契 約 が終 了 する日 。

各Software Bladeのライセンス情 報を表 示 するには

ステップ	手 順
1	セキュリティゲートウェイまたはSecurity Management Serverを選 択します。

ステップ	手順
2	下 のSummaryタブで、オブジェクト のLicense Status (例:OK) をクリックします。 Device & License Informationウィンドウが開きます。各Software Bladeの基 本 的 なオブジェクト 情 報 およびLicense Status、ライセンスExpiration Date、重 要 なクォータ情 報 (Additional Infoカラム) が表 示されます。 注 : ■ クォータ情 報 、クォータに依 存 するライセンスステータス、およびブレード 情 報 メッセージは、R80以 降 でのみサポートされています。 ■ SKUのツールチップはプロダクト 名 です。

Software BladeのLicense Statusに指 定 できる値 は次 のとおりです。

ステータス	説 明
Active	Software Bladeが有 効 で、ライセンスも有 効 です。
Available	Software Bladeは非 アクティブで、ライセンスは有 効 です。
No License	Software Bladeは有 効 ですが、ライセンスが無 効 です。
Expired	Software Bladeは有 効 ですが、ライセンスが失 効 しています。
About to Expire	Software Bladeは有 効 ですが、ライセンスの有 効 期 限 は30日 (デフォルト) 以内 (評 価 ライセンスの場 合 は7日 以 内) です。
Quota Exceeded	Software Bladeはアクティブであり、ライセンスも有 効 ですが、関 連 オブジェクト (Security Gateway、ファイル、仮 想 システムなど、ブレードによって異 なる) のクォータを超 過 しています。
Quota Warning	Software Bladeはアクティブで、ライセンスも有 効 ですが、このブレード のオブジェクト 数 がライセンス枠 の90%(デフォルト) 以 上 です。
N/A	ライセンス情 報 は利 用 できません。

VSXのライセンス情 報 の表 示

仮 想 システムまたは仮 想 ルータ オブジェクト のライセンスを表 示 すると、SmartConsoleにエラーが表 示されます。

VSXのライセンス情 報 を見 るには

VSXゲート ウェイまたはVSXクラスタオブジェクト を選 択 します (バーチャルシステムまたはバーチャ ルルータのオブジェクト は選 択 しません) 。

SmartConsoleでのライセンスのモニタ

ライセンスに関する問題を把握するために、以下のオプションを使用できます。

オプション	説明
License Status表示	特定のSecurity Management Server、Security Gateway、またはLog Serverオブジェクトごとに、Software Bladesのライセンス情報を確認およびエクスポートできます。
License Statusレポート	Security Management Server、Security Gateway、またはLog Serverで設定されたすべてのオブジェクトのフィルタとライセンスのステータス情報を確認およびエクスポートできます。
License Inventoryレポート	設定されたすべてのSecurity Management Server、Security Gateway、またはLog Serverオブジェクトのフィルタおよびライセンス情報を確認およびエクスポートできます。

SmartEvent Software Bladeでは、SmartConsoleの**Logs & Events**ビューから、**License Status**と**License Inventory**の情報をカスタマイズすることができます。

また、Security Management ServerのSmartEventブレードを有効にしなくても、SmartConsoleの**Gateways & Servers**ビューでライセンス情報を見ることも可能です。

SmartConsoleのGateways & Serversビューを使用すると、*ライセンス インベントリ*レポートを表示およびエクスポートできます。

ステップ	手順
1	ゲートウェイ & サーバビューから [License Inventory] レポートを表示します: 1. SmartConsoleの左側のナビゲーションパネルから、**Gateways & Servers**をクリックします。 2. 上部のツールバーから、**Actions** >**License Report** をクリックします。 3. **SmartView**が読み込まれ、このレポートが表示されるのを待ちます。 デフォルトでは、このレポートには以下の内容が含まれます。 ■ *インベントリページ*: ブレード名、デバイス名、ライセンスステータス ■ *デバイス別ライセンスページ*: デバイス名、ライセンスステータス、CK、SKU、アカウントID、サポートレベル、次回有効期限
2	ゲートウェイ & サーバビューから [License Inventory] レポートをエクスポートします: 1. 右上の**Options**ボタンをクリックします。 2. 該当するエクスポートオプション - **Export to Excel**または**Export to PDF**を選択します。

SmartConsole の [Logs & Events] ビューでは、*ライセンス ステータス*レポートを表 示 、フィルタリング、およびエクスポート できます。

ステップ	手 順
1	ログとイベント ビューからライセンス ステータス レポートを表 示します: 1. SmartConsoleで、左 のナビゲーションパネルからLogs & Events 2. 上 部 で、New Tabまたは[+]をクリックして、新しいタブを開きます。 3. 左 側 のセクションで、Viewsをクリックします。 4. レポート のリスト で、License Statusをダブルクリックします。 5. SmartViewが読 み込 まれ、このレポート が表 示 されるのを待 ちます。 デフォルト では、このレポート には以 下 の内 容 が含 まれます。 ■ 設 定 されているオブジェクト の名 前 、各 オブジェクト のライセンス状 況 、CK、SKU、アカウント ID、サポート レベル、次 の有 効 期 限
2	Logs & Events ビューの [License Status] レポート をフィルタリングします: 1. 右 上 のOptionsボタン> View Filterをクリックします。 Edit View Filterウィンドウが開きます。 2. Fieldを選 択 し、結 果 をフィルタリングします。例: Device Name、License Status、Account ID 3. 論 理 演 算 子 - Equals、Not Equals、またはContainsを選 択 します。 4. フィルタの値 を選 択 または入 力 します。 注 - フィルタを削 除 するには、Xアイコンをクリックします。 5. オプション: +アイコンをクリックして、追 加 のフィルタを設 定 します。 6. クリックOKをクリックして、設 定 されたフィルタを適 用 します。 設 定 されたフィルタに基 づき、レポート がフィルタリングされます。
3	Logs & Eventsビューのライセンスステータスレポート をエクスポートします: 1. 右 上 のOptionsボタンをクリックします。 2. 該 当 するエクスポート オプション - Export to ExcelまたはExport to PDFを選 択 します。

SmartConsole の [Logs & Events] ビューでは、*ライセンス インベントリレポート*を表 示 、フィルタリング、およびエクスポート できます。

ステップ	手 順
1	Logs & Events ビューからライセンス インベントリレポートを表 示 : 1. SmartConsoleで、左 のナビゲーションパネルから**Logs & Events** 2. 上 部 で、**New Tab**または**[+]**をクリックして、新しいタブを開きます。 3. 左 側 のセクションで、**Reports**をクリックします。 4. レポート のリスト で、**License Inventory**をダブルクリックします。 5. **SmartView**が読 み込 まれ、このレポート が表 示 されるのを待 ちます。 デフォルト では、このレポート には以 下 の内 容 が含 まれます。 ■ *インベントリページ* : ブレード 名 、デバイス名 、ライセンスステータス ■ *デバイス別 ライセンスページ* : デバイス名 、ライセンスステータス、CK、SKU、アカウントID、サポートレベル、次 回 有 効 期 限
2	Logs & Events ビューのライセンス インベントリレポートをフィルタリング : 1. 右 上 の**Options**ボタン**> Report Filter**をクリックします。 **Edit Report Filter**ウィンドウが開きます。 2. **Field**を選 択 し、結 果 をフィルタリングします。例 : **Blade Name**、**Device Name**、**License Overall Status**、**Account ID** 3. 論 理 演 算 子 - **Equals**、**Not Equals**、または**Contains**を選 択 します。 4. フィルタの値 を選 択 または入 力 します。 注 - フィルタを削 除 するには、**X**アイコンをクリックします。 5. オプション : **+** アイコンをクリックして、追 加 のフィルタを設 定 します。 6. クリック**OK**をクリックして、設 定 されたフィルタを適 用 します。 設 定 されたフィルタに基 づき、レポート がフィルタリングされます。
3	Logs & Events ビューのライセンスインベントリレポートをエクスポートします : 1. 右 上 の**Options**ボタンをクリックします。 2. 該 当 するエクスポート オプション - **Export to Excel**または**Export to PDF**を選 択 します。

ライセンスまたはクォータの変 更

SmartConsole GUIクライアント は、ライセンスやクォータの変 更 をリアルタイムで認 識 しません。その結 果 、Security Management Serverでライセンスクォータを超 えた場 合 でも、**'License quota Exceeded'** のアラート がすぐにポップアップ表 示 されません。

ライセンスの変更を確認するには

1. SmartConsoleでSecurity Management Serverにアクセスします。
2. 左側のナビゲーションパネルで**Logs & Events**をクリックします。
3. 上部から [+] をクリックすると、新しいタブが開きます。
4. **Compliance**ビューを開きます(詳細はsk120256 - ATRG: Compliance Blade (R80.10 and higher)を参照) 。

エンタイトルメントまたはコンプライアンスにおけるクォータデータの変更は、次の実行後に更新されます:

- コンプライアンスミッドナイトスキャン
- ライセンス変更
- Security Management Server上での'`cpstop ; cpstart`'コマンド実行

セキュリティゲート ウェイインジケータ

管 理 者 はSmartConsoleで複 数 のセキュリティゲート ウェイを管 理 します。ゲート ウェイ & サーバ ビューの [セキュリティゲート ウェイ インジケータ] 機 能 を使 用 すると、管 理 者 はどのJumbo Hotfix Accumulatorがインスト ールされているかを確 認 し、すべてのセキュリティゲート ウェイが推 奨 される最 新 バージョンであることを確 認 できます。

ゲート ウェイ & サーバービューの [**Version**] カラムには、各 セキュリティゲート ウェイに現 在 インスト ールされているJumbo Hotfix Accumulatorが表 示 されます。**Version**カラム上 にいくと、現 在 インスト ールされているJumbo Hotfix Accumulatorが推 奨 されていない場 合 、インスト ールに推 奨 される Jumbo Hotfix Accumulatorを示 すメッセージが表 示 されます。

Versionカラムには、セキュリティゲート ウェイのステータスに基 づいたインジケータが表 示 されます:

- **カラーインジケータなし**:
  - セキュリティゲート ウェイが更 新 されます。最 新 のJumbo Hotfix Accumulatorがセキュリ ティゲート ウェイにインスト ールされています。
  - セキュリティゲート ウェイにインスト ールされているJumbo Hotfix Accumulatorが最 新 で はありません。インスト ールに推 奨 されるJumbo Hotfix Accumulatorを示 すメッセージが 表 示 されます。
- **黄 色 表 示** - Jumbo Hotfix AccumulatorのTakeが古 すぎるため、推 奨 のJumbo Hotfix Accumulatorにアップグレードする必 要 があります。
- **赤 色 インジケータ** - セキュリティゲート ウェイにインスト ールされているバージョンはサポート され ていません。
- **グレー表 示** - セキュリティゲート ウェイに関 する利 用 可 能 な情 報 がありません。この場 合 、グ レーのインジケータが表 示 されます:
  - セキュリティゲート ウェイのバージョンは、この機 能 をサポートしていません。
  - セキュリティゲート ウェイがCheck Pointのダウンロード センターに1か月 以 上 接 続 されて いません。
  - Check Point Download Centerでは、セキュリティゲート ウェイのアップデート が許 可 され ません。
  - セキュリティゲート ウェイにライセンス/コントラクト がありません。

インジケータの例 外 リストについては、sk182159を参 照 してください。

セキュリティゲート ウェイのインジケータは、Gateways & Serversビューの下 部 にある各 セキュリティ ゲート ウェイの**Summary**タブにも表 示 されます。

Gateways & Serversビューは、ゲート ウェイインジケータに基 づいてフィルタリングできます。これを行 うには、ツールバー上 部 のメニューからフィルタアイコン を選 択 し、**version warning**を選 択 しま す。可 能 なオプションから選 択 します:

- **None**- カラーインジケータのないセキュリティゲート ウェイ
- **Unsupported**- 赤 色 インジケータ付 きセキュリティゲート ウェイ
- **Alert**- 黄 色 のインジケータ付 きセキュリティゲート ウェイ
- **N/A**- グレーインジケータ付 きセキュリティゲート ウェイ

注

- クラスタメンバの表 示 は、セキュリティクラスタオブジェクト に対してではなく、各 クラスタメンバに対して独 立して表 示されます。
- VSXゲート ウェイをアップグレード すると、関 連 するすべての仮 想 ゲート ウェイもアップグレード されます。

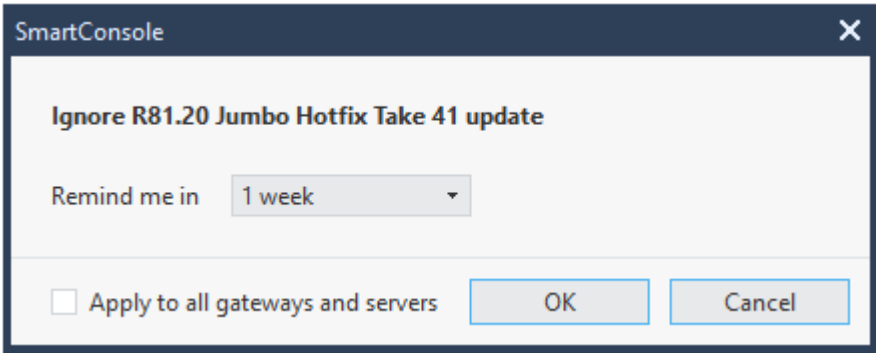
セキュリティゲート ウェイへの推 奨 Takeのインスト ール

セキュリティゲート ウェイにカーソルを合 わせると、セキュリティゲート ウェイにインスト ールするJumbo Hotfix Accumulatorを示 すメッセージが表 示されます。

セキュリティゲート ウェイへのJumbo Hotfix Accumulatorのインスト ールを延 期 するには

1. メッセージ内 の**Options**ボタンをクリックします。

   推 奨されるJumbo Hotfix Accumulatorのテイク番 号 の名 前 でウィンド ウが開きます。



2. このウィンド ウでは、将 来 のインスト ール日 のリマインダーを設 定 できます。ド ロップダウンメニューから、将 来 の再 スケジューリングに必 要 な時 間 を選 択します。**Apply to all gateways and servers**チェックボックスをオンにすると、Hotfixが適 用されるすべてのセキュリティゲート ウェイとサーバーリマインダーが設 定されます。
3. **OK**をクリックします。

関 連 するすべてのセキュリティゲート ウェイとサーバーのインジケータがオフになります。

推 奨されるJumbo Hotfix Accumulatorをセキュリティゲート ウェイにインスト ールするには

1. **Open Installation Window**ボタンをクリックします。

   Install Jumbo/Hotfixウィンド ウが開きます。

2. **Hotfix/Jumbo**セクションで、以下のいずれかを選択します。

   - **Install the Recommended Hotfix/Jumbo**

     または

     Install a Specific Hotfix/Jumbo

     a. バージョン番号/Hotfixファイル名を入力します。

     b. テキストボックスの横にある検索アイコンをクリックします。

     このプロセスにより、Check Pointのサーバからパッケージがダウンロードできるようになります。

3. **Gateways**セクションで、このインストールで選択したセキュリティゲートウェイを参照してください。

   注 - 複数のセキュリティゲートウェイまたはクラスタメンバにパッケージをインストールするには、[Gateways & Servers]ビューに移動し、**CTRL**キーを押したままにして、必要なセキュリティゲートウェイとクラスタメンバをすべて選択します。次に、上部のツールバーメニューから**Actions**をクリックし、**Install Jumbo/Hotfix**を選択します。

4. **Settings**セクションで、ハイアベイラビリティクラスタに該当するオプションを選択します:

   - **Install on all cluster members**- 選択したパッケージをこのクラスタのすべてのメンバ(アクティブおよびスタンバイ)にインストールします。これはフェイルオーバーをクラスタ化し、トラフィックを中断させる可能性があります。
   - **Install on non-active members only**- 選択したパッケージをスタンバイクラスタメンバにのみインストールします。
     - **Once installation is complete, turn non-active member to active**- スタンバイクラスタメンバのクラスタ状態をアクティブに変更します。

5. **Download package timing**セクション - 検証プロセス中にパッケージをダウンロードする場合は、このチェックボックスを選択します:**Download/Deliver package to Security Gateways as part of verification**このチェックボックスを選択しない場合、検証プロセスが最初に実行され、その後、別のアクションとしてファイルがダウンロードされます。

6. **Advanced** セクションで、セキュリティゲートウェイがパッケージをダウンロードするソースを選択します:

   - **Automatic**- パッケージがパッケージリポジトリにある場合、管理サーバはパッケージをセキュリティゲートウェイに転送します。パッケージリポジトリにパッケージが存在しない場合、セキュリティゲートウェイはCheck Point Cloudからパッケージをダウンロードします。
   - **Gateway**- セキュリティゲートウェイは、Check Point Cloudからパッケージをダウンロードします。セキュリティゲートウェイはインターネットに接続されている必要があります。

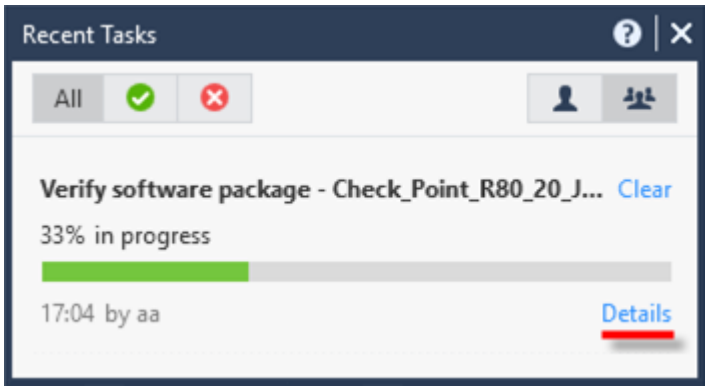
- **Management**- セキュリティゲート ウェイが管 理 サーバからパッケージをダウンロードしま す。

7. 一 番 下 で、**Verify**をクリックします。

   検 証 が始 まります。検 証 プロセスでは、選 択 したHotfixがターゲット にインスト ールできることを確 認 します。検 証 プロセスでは、このパッケージがインスト ールされている他 のHotfixを上 書 きしないこと、およびプロセスが完 了 するまでに十 分 な空 きディスク容 量 があることを確 認 しま す。

   検 証 プロセスの進 行 状 況 を確 認 するには、SmartConsoleの左 下 にある**Tasks**のビューを開 き、**Details**をクリックします。

   例 :



8. クリック**Install**。
9. セントラルデプロイメント で、Access Control Policyがインスト ールされていることを確 認 しま す。
10. インスト ールが完 了 したら、対 象 のセキュリティゲート ウェイおよびクラスタに該 当 する脅 威 対 策 ポリシーをインスト ールする必 要 があります。

ホットフィックスとバージョンアップの一元的な展開

はじめに

SmartConsoleのCentral Deploymentを使用して、次を一括で展開します。

- セキュリティゲートウェイおよびクラスタメンバへのJumbo Hotfix AccumulatorとHotfix。
- セキュリティゲートウェイ、クラスタメンバ、ログサーバ、セカンダリマネジメントのパッケージをアップグレードします。
- Jumbo Hotfix AccumulatorsとHotfixをアンインストールします。

HotfixまたはUpgrade Packageの展開は、以下からも実行できます。

- Check Point Cloud。
- Management Server上のパッケージリポジトリ。

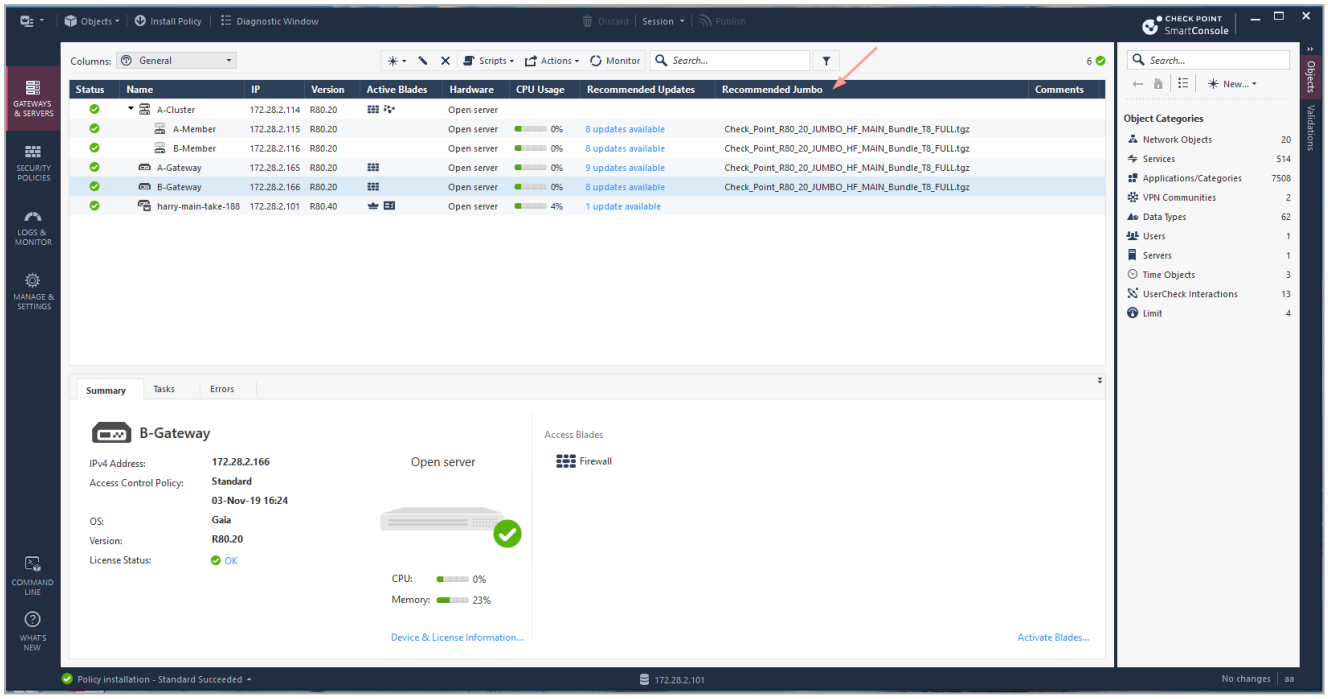
  まず、該当するパッケージをパッケージリポジトリにアップロードする必要があります。参照: *パッケージリポジトリへのパッケージの追加 (247ページ)*。

APIを通じてセントラルデプロイメントを使用するには*Check Point Management API Reference*。

ベストプラクティス - ターゲットから管理サーバへの接続性が、ターゲットからクラウドへの接続性よりも優れている場合、またはターゲットがトラフィックで過負荷になっている場合は、管理サーバ上のパッケージリポジトリを使用します。

注 - セキュリティゲートウェイとクラスタメンバは最大30台まで選択できますが、インストールは同時に10台のターゲットにしか行えません。Management Serverは、キューの10番目以上に各ターゲットを入れます。ターゲットの1つでインストールが完了するたびに、Management Serverはキュー内の次のターゲットにインストールを行います。

一部のSecurity Gatewayには、推奨されるHotfixがあります。**Gateways & Servers**ビューの**Recommended Jumbo**カラムを参照してください。



推奨Jumbo Hotfix Accumulatorまたは特定のJumbo Hotfix Accumulator Takeを展開することができます。

事前準備

Central Deploymentを使用するには:

- 管理者は、管理サーバのSmartUpdate書き込み権限が必要です。
- 対象のセキュリティゲートウェイとクラスタメンバ、または管理サーバに、CPUSE デプロイメントエージェントの最新ビルドをインストールする必要があります。
- Management Serverと対象のSecurity Gatewayおよびクラスタメンバとの間で、すでにSICが確立されている必要があります。
- 対象のセキュリティゲートウェイとクラスタメンバにポリシーがインストールされている必要があります。
- 選択できるのはフルクラスタのみです(クラスタメンバを1人選択することはできません) 。

Check Point Cloudから直接Central Deploymentを使用するには:

1. Management Serverは、Check Point Cloudに接続できる状態である必要があります。
2. 対象のセキュリティゲートウェイとクラスタメンバは、Check Point Cloudに接続できる状態である必要があります。

制限事項

- R80.30、R80.20、R80.10からのアップグレード(これらのバージョンから上位バージョンへのアップグレードには、CPUSEインプレースアップグレードを使用)
- セントラルデプロイメントはサポートしていません:
  - SmartConsoleからプロキシサーバを経由してSecurity Management Serverに接続します。
    この場合、該当するAPIコマンドを使用します。
  - ClusterXLを不可共有モードで使用する。
  - VRRPクラスタ。
  - Maestroのセキュリティグループ。
  - スケーラブルシャーシ 40000 / 60000 のセキュリティグループ。
  - ElasticXLクラスタ。
  - Gaia Embeddedオペレーティングシステムを実行するCentrally Managed Quantum Spark Applianceの場合:
    - Check Point Cloudからパッケージをダウンロードします。必要なパッケージをSecurity Management Serverのパッケージリポジトリに手動で追加する必要があります。
    - SmartConsole Central デプロイメントを使用して、Quantum Sparkアプライアンスに既にインストールされているファームウェアパッケージよりも低いビルド番号の同じバージョンのファームウェアパッケージをインストールする場合、"Verify "アクションはファームウェアのビルド番号を比較しません。そのため、SmartConsoleには「パッケージはインストールに有効です」と表示されますが、実際にはインストールは失敗します。
  - マルチドメインサーバでは、SmartConsoleはグローバルドメイン、またはマルチドメインサーバのコンテキストに接続されていました。

インストール

パッケージリポジトリへのパッケージの追加

1. 左側のナビゲーションパネルで**Manage & Settings**をクリックします。
2. 左側のツリーから、**Package Repository** をクリックします。
3. **New**をクリックして、次のオプションのいずれかを選択します。
   - **Download from cloud**- Check Point Cloudから**Package Repository**にパッケージをダウンロードするには、パッケージのCPUSE識別子を貼り付けて、**Download**をクリックします。

- **Upload from local**- デバイスから**Package Repository**にパッケージをアップロードするには、該当するパッケージを参照し、**Open**をクリックします。

ダウンロードまたはアップロードが完了すると、SmartConsole > **Package Repository**ビューの**Manage & Settings**ウィンドウにパッケージが表示されます。

注:

- 一度に1つのパッケージをリポジトリに追加します。
- Gaia Embedded OS**R80.20.xx以降**を実行するQuantum Spark Applianceの場合、特別な**TAR**パッケージ(ファームウェアイメージと必要な設定ファイル `hf.config`を含む) をダウンロードし、**"Upload from local"** オプションを使用する必要があります。
- マルチドメイン環境で**Package Repository**にパッケージをアップロードする場合:
  - パッケージをグローバルドメインにアップロードすることができます。この場合、すべてのドメインからアップロードされたパッケージを確認し、希望のドメインにインストールすることができます。
  - パッケージを特定のドメインにアップロードすることができます。この場合、パッケージを確認し、特定のドメインにのみインストールすることができます。

複数のセキュリティゲートウェイまたはクラスタメンバへのHotfixまたはアップグレードパッケージのインストール

警告 - Gaia Embedded OSを実行するQuantum Sparkアプライアンスにファームウェアをインストールする前に、USBポートから外部ストレージを取り外す必要があります(最低限、外部スト レージにQuantum Sparkアプライアンス用のファームウェアイメージが含まれていないことを確認してください) 。

ベストプラクティス - HotfixやアップグレードパッケージをSecurity Management Serverに集中的にデプロイメントする場合、管理下のGaiaサーバからのステータスレポートに依存します。そのため、Hotfixやアップグレードパッケージをインストールするまえに、Gaiaサーバが起動してから2分間待つことをお勧めします。

1. 左側のナビゲーションパネルで**Gateways & Servers**をクリックします。
2. 展開先のセキュリティゲートウェイまたはクラスタメンバを選択します。

   対象を複数選択する場合は、**CTRL**キーを長押しして選択します。

   クラスタメンバをアップグレードするには、クラスタオブジェクトを選択します。
3. ツールバーのメニューから**Actions**をクリックし、以下のオプションのいずれかを選択します:

   - **Install Hotfix/Jumbo**
   - **Version Upgrade**

   Install Hotfixまたは**Version Upgrade**ウィンドウが開き、選択したターゲットと対応する推奨Hotfixまたはアップグレードパッケージに関する情報が表示されます。
4. **「Hotfix/Jumboのインストール」を選択した場合は、Hotfix/Jumboセクションで、以下のいずれかのオプションを選択してください:**

- **Install the Recommended Hotfix/Jumbo**

  または

- **Install a Specific Hotfix/Jumbo**

  注 - 選択したターゲットに推奨されるJumbo Hotfix Accumulatorがない場合、このオプションはグレーアウトされます。推奨されるJumbo Hotfix Accumulatorが選択された一部のターゲットにのみ適用される場合、それらのターゲットに対してのみデプロイメントが行われます。

  a. Hotfixのファイル名を入力してください。

     該当するSKアーティクルからHotfixファイル名をコピーして、**Install Specific Hotfix**テキストボックスに入力することができます。

     注 - "**Install a Specific Hotfix/Jumbo**" フィールドを使用してGaia Embedded OS **R80.20.xx以降**を実行するQuantum Spark Applianceにファームウェアパッケージをインストールします。管理サーバは、同じメインバージョンに基づくファームウェアパッケージをJumbo Hotfixと見なします。例えば、すべてのファームウェアパッケージR81.10.XXは、メインバージョンR81.10をベースにしています。

     セキュリティゲートウェイR80.20の例：

     • Ongoing Take

Product	Take	Date	CPUSE Online Identifier	SmartConsole package
Security Gateway / Standalone	Jumbo HF Take_127	03 Dec 2019	Check_Point_R80_20_JUMBO_HF_Bundle_T127_sk137592_Security_Gateway_and_Standalone_2_6_18_FULL.tgz	(EXE) Build 081
Security Management			Check_Point_R80_20_JUMBO_HF_Bundle_T127_sk137592_Security_Management_3_10_FULL.tgz	

  b. テキストボックスの横にある検索アイコンをクリックして、利用可能なパッケージを検索します。

バージョンのアップグレードを選択した場合は、バージョンのアップグレード ウィンドウで、以下のいずれかのオプションを選択します：

- **Upgrade to the Recommended Major Version**

  または

- **Upgrade to a Specific Major Version**

  a. バージョン番号を入力します。

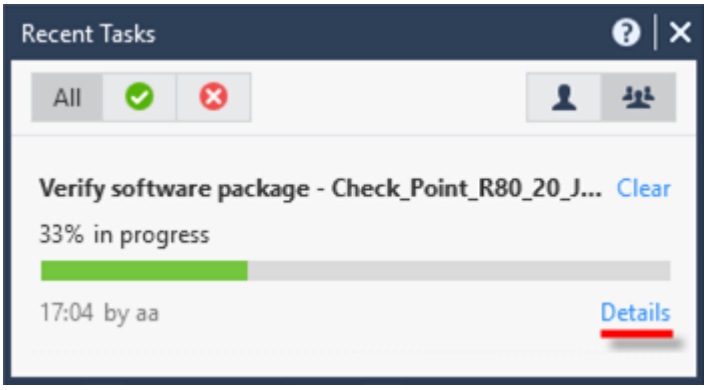
  b. テキストボックスの横にある検索アイコンをクリックして、利用可能なパッケージを検索します。

5. **Gateways**セクションには、パッケージをインストールするために選択したターゲットが表示されます。
6. **Settings**セクションで、ハイアベイラビリティクラスタに該当するオプションを選択します:
   - **Install on all cluster members**- 選択したパッケージをこのクラスタのすべてのメンバ(アクティブおよびスタンバイ)にインストールします。これはフェイルオーバーをクラスタ化し、トラフィックを中断させる可能性があります。
   - **Install on non-active members only**- 選択したパッケージをスタンバイクラスタメンバにのみインストールします。
     - **Once installation is complete, turn non-active member to active**- スタンバイクラスタメンバのクラスタ状態をアクティブに変更します。
7. **Advanced**セクションで、セキュリティゲートウェイがパッケージをダウンロードする場所を選択します:
   - **Automatic**- パッケージがパッケージリポジトリにある場合、管理サーバはパッケージをセキュリティゲートウェイに転送します。パッケージリポジトリにパッケージが存在しない場合、セキュリティゲートウェイはCheck Point Cloudからパッケージをダウンロードします。
   - **Gateway**- セキュリティゲートウェイは、Check Point Cloudからパッケージをダウンロードします。セキュリティゲートウェイはインターネットに接続されている必要があります。
   - **Management**- セキュリティゲートウェイがManagement Serverからパッケージをダウンロードします。
8. 一番下で、**Verify**をクリックします。

   検証プロセスが始まります。検証プロセスでは、選択したHotfixまたはアップグレードパッケージがターゲットにインストールできることを確認します。検証プロセスでは、このパッケージがインストールされている他のHotfixを上書きしないこと、およびプロセスが完了するまでに十分な空きディスク容量があることを確認します。

   検証プロセスの進行状況を確認するには、SmartConsoleの左下にある**Tasks**のビューを開き、**Details**をクリックします。

   例:



9. クリックInstall。
10. セントラルデプロイメントは、アクセスコントロールポリシーがインストールされていることを確認します。
11. インストールが完了したら、対象のセキュリティゲートウェイおよびクラスタに該当する脅威対策ポリシーをインストールする必要があります。

注

- ターゲットによって推奨されるHotfixまたはアップグレードパッケージが異なる場合は、各ターゲットに該当する推奨Hotfixまたはアップグレードパッケージが設定されます。
- Gaia Embeddedオペレーティングシステムを実行するQuantum Sparkアプライアンスにファームウェアをインストールする前に、USBポートから外部ストレージを取り外す必要があります(最低限、Quantum Sparkアプライアンス用のファームウェアイメージが含まれていないことを確認してください) 。

HotfixまたはJumbo Hotfix Accumulatorのアンインストール

HotfixまたはJumbo Hotfix Accumulatorをアンインストールするには

1. 左側のナビゲーションパネルでGateways & Serversをクリックします。
2. 展開先のセキュリティゲートウェイまたはクラスタメンバを選択します。

   対象を複数選択する場合は、CTRLキーを長押しして選択します。

   クラスタメンバにパッケージをアンインストールするには、クラスタオブジェクトを選択します。
3. ツールバーのメニューから、Actionsをクリックし、Uninstall Hotfix/Jumboを選択します。

   Uninstall Hotfix/Jumboウィンドウが開きます。
4. Hotfix/Jumboセクションで、アンインストールするHotfix/Jumboを入力します。
5. Gatewaysセクションで、HotfixまたはJumbo Hotfix Accumulatorのアンインストール時に選択した対象を確認してください。
6. 一番下で、Verifyをクリックします。

検証が始まります。検証プロセスでは、選択したHotfixまたはJumbo Hotfix Accumulatorがターゲットからアンインストールできるように、必要な条件がすべて満たされていることを確認します。

検証プロセスの進行状況を確認するには、SmartConsoleの左下にある**Tasks**のビューを開き、**Details**をクリックします。

7. **Uninstall**をクリックします。

セントラルデプロイメントによるクラスタのアップグレード方法

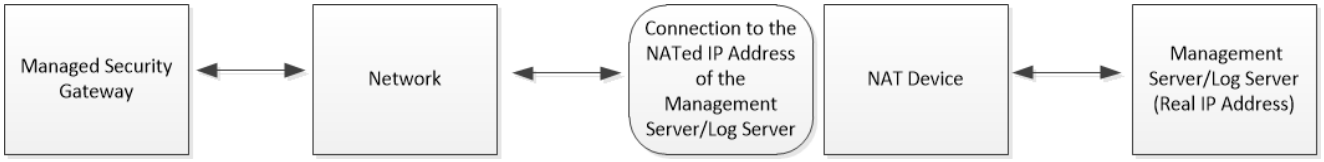
セントラルデプロイメントを使用して、ハイアベイラビリティモードのClusterXLまたはVSXクラスタ(非VSLS)のすべてのメンバにソフトウェアパッケージをインストールする場合、セントラルデプロイメントは次の手順に従います:

1. クラスタメンバの状態が有効であることを確認します(アクティブとスタンバイ)。
2. クラスタのアクセスコントロールポリシーを準備します。
   a. クラスタオブジェクトのバージョンを変更します。
   b. 該当するコンフィギュレーション設定とアクセスコントロールポリシーを変更します。
3. スタンバイクラスタメンバを新しいバージョンにアップグレードします。
4. マルチバージョンクラスタ(MVC)を実行します。
   a. アップグレードされたクラスタメンバがスタンバイまたはレディ状態であることを確認します。
   b. アップグレードされたクラスタメンバのいずれかにクラスタフェイルオーバーを実行します。
5. アクティブだったクラスタメンバをアップグレードします。
6. クラスタメンバの状態が有効であることを確認します(アクティブとスタンバイ)。

NATed IPアドレスで管理サーバまたはログサーバにアクセスするセキュリティゲートウェイの設定

セキュリティゲートウェイは、ポリシーの取得やログの送信のために、サーバのNATed IPアドレスでSecurity Management ServerまたはLog Serverにアクセスするように設定することができます。

次の図は、この流れを説明しています。



手順:

1. Security Gateway/各クラスタメンバのコマンドラインに接続します。
2. エキスパートモードにログインします。
3. VSXゲートウェイ/各VSXクラスタメンバで、該当するバーチャルシステムのコンテキストに移動します。

   ```
   vsenv <VSID>
   ```

4. 該当するコマンドを実行します(この変更は再起動後も反映されます)。

   a. Security Gateway / クラスタメンバが、管理サーバまたはログサーバの**パブリック(NATed)** IPアドレス(これがデフォルトの動作です)にのみ接続するようにするには、以下を実行します。

   ```
   ckp_regedit -a SOFTWARE\\CheckPoint\\FW1 FORCE_NATTED_IP
   -n 1
   ```

   b. セキュリティゲートウェイ/クラスタメンバが、Management ServerまたはLog Serverの**実際の**IPアドレスのみに接続するようにするには、以下を実行します。

   ```
   ckp_regedit -a SOFTWARE\\CheckPoint\\FW1 FORCE_NATTED_IP
   -n 0
   ```

   注:
   - この変更は再起動後も反映されます。
   - クラスタでは、すべてのクラスタメンバを同じ方法で設定する必要があります。

5. FWD処理をプロセスを再開します。

   sk97638 > セクション「*インフラストラクチャプロセス*」の説明を参照。

セキュリティゲートウェイの暗黙ルールまたはカーネルテーブルの設定

はじめに

管理者は、SmartConsoleでセキュリティポリシーやその他のインスペクション設定を行います。

ポリシーのインストール時に、Management Serverは該当するファイルを作成し、対象のセキュリティゲートウェイに転送します。

Management Serverではこれらのファイルを次に基づいて作成します。

- SmartConsoleのセキュリティポリシー
- SmartConsoleのグローバルプロパティ
- セキュリティゲートウェイのプロパティ
- 様々なネットワークプロトコルのインスペクションを制御するManagement Server上の複数の設定ファイル

Management Server上でこれらの設定ファイルを変更し、ネットワークにおけるインスペクションを細かく調整することが可能です(Check Point INSPECTの言語) 。

これらの設定ファイルには、大きく分けて2つのカテゴリがあります。

- Management Serverと同じソフトウェアバージョンを持つSecurity Gateway用のファイル。
- Management Serverより下位のソフトウェアバージョンを持つSecurity Gateway用のファイル。このカテゴリは「後方互換性」と呼ばれます。

設定ファイル

ファイル名	コントロール	位置情報
`user.def`	ユーザが定義した暗黙のルール。	参照: *Management Serverの'user.def'ファイルの場所 (257ページ)*
`implied_rules.def`	デフォルトの暗黙ルール。	参照: *Management Server上の'implied_rules.def'ファイルの場所 (258ページ)*
`table.def`	各種カーネルテーブルの定義。	参照: *Management Server上の'table.def'ファイルの場所 (260ページ)*

ファイル名	コントロール	位置情報
crypt.def	VPN暗号化マクロ。	参照: *管理サーバ上の'crypt.def'ファイルの場所 (262ページ)*
vpn_table.def	VPNデータを保持する様々なカーネルテーブルの定義。 例えば、VPNタイムアウト、VPNトンネル数、特定のカーネルテーブルをクラスタメンバ間で同期させるかどうか、などです。	参照: *Management Server上の「vpn_table.def」ファイルの場所 (264ページ)*
communities.def	X11 サーバ(X Window System)トラフィック用のVPN暗号化マクロ。	参照: *管理サーバ上の'communities.def'ファイルの場所 (268ページ)*
base.def	各種ネットワークプロトコルのパケットインスペクションの定義。	参照: *管理サーバ上の'base.def'ファイルの場所 (270ページ)*
dhcp.def	DHCPトラフィックのパケットインスペクションの定義 - DHCP Request、DHCP Reply、DHCP Relay。	参照: *Management Server上の'dhcp.def'ファイルの場所 (272ページ)*
gtp.def	GTP(GPRS Tunnelling Protocol)トラフィックのパケットインスペクションの定義。	参照: *Management Serverの'gtp.def'ファイルの場所 (274ページ)*

設定手順

1. セキュリティ管理サーバのコマンドラインに接続します。
2. エキスパートモードにログインします。
3. 現在のファイルをバックアップします。

   ```
   cp -v /<Full Path to File>/<File Name>{,_BKP}
   ```

   例:

   ```
   cp -v $FWDIR/conf/user.def.FW1{,_BKP}
   ```

4. 現在のファイルを編集します:

   ```
   vi /<Full Path to File>/<File Name>
   ```

   例:

   ```
   vi $FWDIR/conf/user.def.FW1
   ```

5. 該当するSKの記事、またはCheck Pointの指示に従って、該当する変更を行います。
6. 変更内容をファイルに保存し、エディタを終了します。
7. SmartConsoleでSecurity Management Serverにアクセスします。
8. SmartConsoleで、該当するセキュリティゲートウェイまたはクラスタオブジェクトにAccess Control Policyをインストールします。

Management Serverの'user.def'ファイルの場所

'user.def'ファイルには、ユーザが定義した暗黙のルールが含まれています。

重要:

- このファイルは、該当するドメイン管理サーバのコンテキスト内で編集する必要があります。
  必要なコンテキストに移動するには、コマンドを使用します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必要なファイルが存在しない場合は、`$FWDIR/conf/user.def.FW1`ファイルのコピーを作成し、名前を変更して編集します。

R82 Security Management Server上のファイルの場所:

対象セキュリティゲートウェイのバージョン	ファイルの場所
R82	`$FWDIR/conf/user.def.FW1`
R81.20	`$FWDIR/conf/user.def.R8120CMP`
R81.10	`$FWDIR/conf/user.def.R8120CMP`
Quantum Spark Appliance 1500 / 1600 / 1800上のR81.10.x	`$FWDIR/conf/user.def.SFWR81CMP`
R81	`$FWDIR/conf/user.def.R8120CMP`
R80.40	`$FWDIR/conf/user.def.R8040CMP`
MaestroのR80.30SP	`$FWDIR/conf/user.def.R8040CMP`
R80.30	`$FWDIR/conf/user.def.R8040CMP`
MaestroのR80.20SPまたはスケーラブルシャーシ	`$FWDIR/conf/user.def.R8040CMP`
R80.20	`$FWDIR/conf/user.def.R8040CMP`
Quantum Sparkアプライアンス 1500 / 1600 / 1800のR80.20.x	`$FWDIR/conf/user.def.SFWR80CMP`
R80.10	`$FWDIR/conf/user.def.R8040CMP`
SMBアプライアンス1100 / 1200R / 1400上のR77.20.x	`$FWDIR/conf/user.def.SFWR77CMP`

Management Server上 の'implied_rules.def'ファイルの場 所

'implied_rules.def'ファイルには、デフォルト の暗 黙 のルールが含 まれています。

重 要 :

- このファイルは、該 当 するドメイン管 理 サーバのコンテキスト 内 で編 集 する必 要 があります。
  必 要 なコンテキスト に移 動 するにはコマンドを使 用 します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必 要 なファイルが存 在 しない場 合 は、`$FWDIR/lib/implied_rules.def`ファイルのコピーを作 成 し、名 前 を変 更 して編 集 します。

R82 Security Management Server上 のファイルの場 所 :

対 象 セキュリティゲート ウェイのバージョン	ファイルの場 所
R82	`$FWDIR/lib/implied_rules.def`
R81.20	`/opt/CPR8120CMP-R82/lib/implied_rules.def`
R81.10	`/opt/CPR8120CMP-R82/lib/implied_rules.def`
Quantum Spark Appliance 1500 / 1600 / 1800上 のR81.10.x	`/opt/CPSFWR81CMP-R82/lib/implied_rules.def`
R81	`/opt/CPR8120CMP-R82/lib/implied_rules.def`
R80.40	`/opt/CPR8040CMP-R82/lib/implied_rules.def`
MaestroのR80.30SP	`/opt/CPR8040CMP-R82/lib/implied_rules.def`
R80.30	`/opt/CPR8040CMP-R82/lib/implied_rules.def`
MaestroのR80.20SPまたはスケーラブルシャーシ	`/opt/CPR8040CMP-R82/lib/implied_rules.def`
R80.20	`/opt/CPR8040CMP-R82/lib/implied_rules.def`
Quantum Sparkアプライアンス 1500 / 1600 / 1800のR80.20.x	`/opt/CPSFWR80CMP-R82/lib/implied_rules.def`

対 象 セキュリティゲート ウェイのバージョン	ファイルの場 所
R80.10	`/opt/CPR8040CMP-R82/lib/implied_rules.def`
SMBアプライアンス1100 / 1200R / 1400上 の R77.20.x	`/opt/CPSFWR77CMP-R82/lib/implied_rules.def`

Management Server上 の'table.def'ファイルの場 所

'table.def'ファイルには、Security Gateway用 の様 々 なカーネルテーブルの定 義 が含 まれています。

重 要 :

- このファイルは、該 当 するドメイン管 理 サーバのコンテキスト 内 で編 集 する必 要 があります。
  必 要 なコンテキストに移 動 するには、コマンドを使 用 します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必 要 なファイルが存 在 しない場 合 は、`$FWDIR/lib/table.def`ファイルのコピーを作 成 し、名 前 を変 更 して編 集 します。

R82 Security Management Server上 のファイルの場 所 :

対 象 セキュリティゲート ウェイのバージョン	ファイルの場 所
R82	`$FWDIR/lib/table.def`
R81.20	`/opt/CPR8120CMP-R82/lib/table.def`
R81.10	`/opt/CPR8120CMP-R82/lib/table.def`
Quantum Spark Appliance 1500 / 1600 / 1800上のR81.10.x	`/opt/CPSFWR81CMP-R82/lib/table.def`
R81	`/opt/CPR8120CMP-R82/lib/table.def`
R80.40	`/opt/CPR8040CMP-R82/lib/table.def`
MaestroのR80.30SP	`/opt/CPR8040CMP-R82/lib/table.def`
R80.30	`/opt/CPR8040CMP-R82/lib/table.def`
MaestroのR80.20SPまたはスケーラブルシャーシ	`/opt/CPR8040CMP-R82/lib/table.def`
R80.20	`/opt/CPR8040CMP-R82/lib/table.def`

対 象 セキュリティゲート ウェイのバージョン	ファイルの場 所
Quantum Sparkアプライアンス 1500 / 1600 / 1800 のR80.20.x	`/opt/CPSFWR80CMP-R82/lib/table.def`
R80.10	`/opt/CPR8040CMP-R82/lib/table.def`
SMBアプライアンス1100 / 1200R / 1400上 の R77.20.x	`/opt/CPSFWR77CMP-R82/lib/table.def`

管理サーバ上の'crypt.def'ファイルの場所

'crypt.def'ファイルには、VPN暗号化マクロが含まれています。

重要:

- このファイルは、該当するドメイン管理サーバのコンテキスト内で編集する必要があります。
  必要なコンテキストに移動するには、コマンドを使用します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必要なファイルが存在しない場合は、`$FWDIR/lib/crypt.def`ファイルのコピーを作成し、名前を変更して編集します。

R82 Security Management Server上のファイルの場所:

対象セキュリティゲートウェイのバージョン	ファイルの場所
R82	`$FWDIR/lib/crypt.def`
R81.20	`/opt/CPR8120CMP-R82/lib/crypt.def`
R81.10	`/opt/CPR8120CMP-R82/lib/crypt.def`
Quantum Spark Appliance 1500 / 1600 / 1800上のR81.10.x	`/opt/CPSFWR81CMP-R82/lib/crypt.def`
R81	`/opt/CPR8120CMP-R82/lib/crypt.def`
R80.40	`/opt/CPR8040CMP-R82/lib/crypt.def`
MaestroのR80.30SP	`/opt/CPR8040CMP-R82/lib/crypt.def`
R80.30	`/opt/CPR8040CMP-R82/lib/crypt.def`
MaestroのR80.20SPまたはスケーラブルシャーシ	`/opt/CPR8040CMP-R82/lib/crypt.def`
R80.20	`/opt/CPR8040CMP-R82/lib/crypt.def`
Quantum Sparkアプライアンス 1500 / 1600 / 1800のR80.20.x	`/opt/CPSFWR80CMP-R82/lib/crypt.def`

対象セキュリティゲートウェイのバージョン	ファイルの場所
R80.10	`/opt/CPR8040CMP-R82/lib/crypt.def`
SMBアプライアンス1100 / 1200R / 1400上のR77.20.x	`/opt/CPSFWR77CMP-R82/lib/crypt.def`

Management Server上の「vpn_table.def」ファイルの場所

'vpn_table.def'ファイルには、VPNデータを保持する様々なカーネルテーブルの定義が含まれています。

例えば、VPNタイムアウト、VPNトンネル数、特定のカーネルテーブルをクラスタメンバ間で同期させるかどうか、などです。

重要:

- このファイルは、該当するドメイン管理サーバのコンテキスト内で編集する必要があります。
  必要なコンテキストに移動するには、コマンドを使用します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必要なファイルが存在しない場合は、`$FWDIR/lib/vpn_table.def`ファイルのコピーを作成し、名前を変更して編集します。

R82 Security Management Server上のファイルの場所:

対象セキュリティゲートウェイのバージョン	ファイルの場所
R82	`$FWDIR/lib/vpn_table.def`
R81.20	`/opt/CPR8120CMP-R82/lib/vpn_table.def`
R81.10	`/opt/CPR8120CMP-R82/lib/vpn_table.def`
Quantum Spark Appliance 1500 / 1600 / 1800上のR81.10.x	`/opt/CPSFWR81CMP-R82/lib/vpn_table.def`
R81	`/opt/CPR8120CMP-R82/lib/vpn_table.def`
R80.40	`/opt/CPR8040CMP-R82/lib/vpn_table.def`
MaestroのR80.30SP	`/opt/CPR8040CMP-R82/lib/vpn_table.def`
R80.30	`/opt/CPR8040CMP-R82/lib/vpn_table.def`
MaestroのR80.20SPまたはスケーラブルシャーシ	`/opt/CPR8040CMP-R82/lib/vpn_table.def`

対 象 セキュリティゲート ウェイのバージョン	ファイルの場 所
R80.20	`/opt/CPR8040CMP-R82/lib/vpn_table.def`
Quantum Sparkアプライアンス 1500 / 1600 / 1800のR80.20.x	`/opt/CPSFWR80CMP-R82/lib/vpn_table.def`
R80.10	`/opt/CPR8040CMP-R82/lib/vpn_table.def`
SMBアプライアンス1100 / 1200R / 1400上 の R77.20.x	`/opt/CPSFWR77CMP-R82/lib/vpn_table.def`

管理サーバ上の「vpn_route.conf」ファイルの場所

'vpn_route.conf'ファイルには、ドメインベースのサイト間VPNの設定が含まれています。

重要:

- このファイルは、該当するドメイン管理サーバのコンテキスト内で編集する必要があります。
  必要なコンテキストに移動するには、コマンドを使用します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必要なファイルが存在しない場合は、`$FWDIR/conf/vpn_route.conf`ファイルのコピーを作成し、名前を変更して編集します。

R82 Security Management Server上のファイルの場所:

対象セキュリティゲートウェイのバージョン	ファイルの場所
R82	`$FWDIR/conf/vpn_route.conf`
R81.20	`/opt/CPR8120CMP-R82/conf/vpn_route.conf`
R81.10	`/opt/CPR8120CMP-R82/conf/vpn_route.conf`
Quantum Spark Appliance 1500 / 1600 / 1800上のR81.10.x	`/opt/CPSFWR81CMP-R82/conf/vpn_route.conf`
R81	`/opt/CPR8120CMP-R82/conf/vpn_route.conf`
R80.40	`/opt/CPR8040CMP-R82/conf/vpn_route.conf`
MaestroのR80.30SP	`/opt/CPR8040CMP-R82/conf/vpn_route.conf`
R80.30	`/opt/CPR8040CMP-R82/conf/vpn_route.conf`
MaestroのR80.20SPまたはスケーラブルシャーシ	`/opt/CPR8040CMP-R82/conf/vpn_route.conf`
R80.20	`/opt/CPR8040CMP-R82/conf/vpn_route.conf`
Quantum Sparkアプライアンス 1500 / 1600 / 1800のR80.20.x	`/opt/CPSFWR80CMP-R82/conf/vpn_route.conf`

対象セキュリティゲートウェイのバージョン	ファイルの場所
R80.10	`/opt/CPR8040CMP-R82/conf/vpn_route.conf`

管理サーバ上の'communities.def'ファイルの場所

'communities.def'ファイルは、X11サーバ(X Window System)トラフィックのためのVPN暗号化マクロを含んでいます。

重要:

- このファイルは、該当するドメイン管理サーバのコンテキスト内で編集する必要があります。
  必要なコンテキストに移動するには、コマンドを使用します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必要なファイルが存在しない場合は、`$FWDIR/lib/communities.def`ファイルのコピーを作成し、名前を変更して編集します。

R82 Security Management Server上のファイルの場所:

対象セキュリティゲートウェイのバージョン	ファイルの場所
R82	`$FWDIR/lib/communities.def`
R81.20	`/opt/CPR8120CMP-R82/lib/communities.def`
R81.10	`/opt/CPR8120CMP-R82/lib/communities.def`
Quantum Spark Appliance 1500 / 1600 / 1800上のR81.10.x	`/opt/CPSFWR81CMP-R82/lib/communities.def`
R81	`/opt/CPR8120CMP-R82/lib/communities.def`
R80.40	`/opt/CPR8040CMP-R82/lib/communities.def`
MaestroのR80.30SP	`/opt/CPR8040CMP-R82/lib/communities.def`
R80.30	`/opt/CPR8040CMP-R82/lib/communities.def`
MaestroのR80.20SPまたはスケーラブルシャーシ	`/opt/CPR8040CMP-R82/lib/communities.def`
R80.20	`/opt/CPR8040CMP-R82/lib/communities.def`

対象セキュリティゲートウェイのバージョン	ファイルの場所
Quantum Sparkアプライアンス 1500 / 1600 / 1800のR80.20.x	/opt/CPSFWR80CMP-R82/lib/communities.def
R80.10	/opt/CPR8040CMP-R82/lib/communities.def
SMBアプライアンス1100 / 1200R / 1400上のR77.20.x	/opt/CPSFWR77CMP-R82/lib/communities.def

管理サーバ上の'base.def'ファイルの場所

'base.def'ファイルには、様々なネットワークプロトコルのパケットインスペクションの定義が含まれています。

重要:

- このファイルは、該当するドメイン管理サーバのコンテキスト内で編集する必要があります。
  必要なコンテキストに移動するには、コマンドを使用します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必要なファイルが存在しない場合は、`$FWDIR/lib/base.def`ファイルのコピーを作成し、名前を変更して編集します。

R82 Security Management Server上のファイルの場所:

対象セキュリティゲートウェイのバージョン	ファイルの場所
R82	`$FWDIR/lib/base.def`
R81.20	`/opt/CPR8120CMP-R82/lib/base.def`
R81.10	`/opt/CPR8120CMP-R82/lib/base.def`
Quantum Spark Appliance 1500 / 1600 / 1800上のR81.10.x	`/opt/CPSFWR81CMP-R82/lib/base.def`
R81	`/opt/CPR8120CMP-R82/lib/base.def`
R80.40	`/opt/CPR8040CMP-R82/lib/base.def`
MaestroのR80.30SP	`/opt/CPR8040CMP-R82/lib/base.def`
R80.30	`/opt/CPR8040CMP-R82/lib/base.def`
MaestroのR80.20SP、またはスケーラブルシャーシ	`/opt/CPR8040CMP-R82/lib/base.def`
R80.20	`/opt/CPR8040CMP-R82/lib/base.def`

対象セキュリティゲートウェイのバージョン	ファイルの場所
Quantum Sparkアプライアンス 1500 / 1600 / 1800のR80.20.x	/opt/CPSFWR80CMP-R82/lib/base.def
R80.10	/opt/CPR8040CMP-R82/lib/base.def
SMBアプライアンス1100 / 1200R / 1400上のR77.20.x	/opt/CPSFWR77CMP-R82/lib/base.def

Management Server上の'dhcp.def'ファイルの場所

'dhcp.def'ファイルには、DHCPトラフィック(DHCP Request、DHCP Reply、DHCP Relay) のパケットインスペクションに関する定義が含まれています。

重要:

- このファイルは、該当するドメイン管理サーバのコンテキスト内で編集する必要があります。
  必要なコンテキストに移動するには、コマンドを使用します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必要なファイルが存在しない場合は、`$FWDIR/lib/dhcp.def`ファイルのコピーを作成し、名前を変更して編集します。

R82 Security Management Server上のファイルの場所:

対象セキュリティゲートウェイのバージョン	ファイルの場所
R82	`$FWDIR/lib/dhcp.def`
R81.20	`/opt/CPR8120CMP-R82/lib/dhcp.def`
R81.10	`/opt/CPR8120CMP-R82/lib/dhcp.def`
Quantum Spark Appliance 1500 / 1600 / 1800上のR81.10.x	`/opt/CPSFWR81CMP-R82/lib/dhcp.def`
R81	`/opt/CPR8120CMP-R82/lib/dhcp.def`
R80.40	`/opt/CPR8040CMP-R82/lib/dhcp.def`
MaestroのR80.30SP	`/opt/CPR8040CMP-R82/lib/dhcp.def`
R80.30	`/opt/CPR8040CMP-R82/lib/dhcp.def`
MaestroのR80.20SPまたはスケーラブルシャーシ	`/opt/CPR8040CMP-R82/lib/dhcp.def`
R80.20	`/opt/CPR8040CMP-R82/lib/dhcp.def`

対 象 セキュリティゲート ウェイのバージョン	ファイルの場 所
Quantum Sparkアプライアンス 1500 / 1600 / 1800の R80.20.x	`/opt/CPSFWR80CMP-R82/lib/dhcp.def`
R80.10	`/opt/CPR8040CMP-R82/lib/dhcp.def`
SMBアプライアンス1100 / 1200R / 1400上 の R77.20.x	`/opt/CPSFWR77CMP-R82/lib/dhcp.def`

Management Serverの'gtp.def'ファイルの場所

'gtp.def'ファイルには、GTP (GPRS Tunnelling Protocol) トラフィックのパケット インスペクションの定義が含まれています。

重要:

- このファイルは、該当するドメイン管理サーバのコンテキスト内で編集する必要があります。
  必要なコンテキストに移動するには、コマンドを使用します:
  `mdsenv <IP Address or Name of Domain Management Server>`
- 必要なファイルが存在しない場合は、`$FWDIR/lib/gtp.def`ファイルのコピーを作成し、名前を変更して編集します。

R82 Security Management Server上のファイルの場所:

対象セキュリティゲートウェイのバージョン	ファイルの場所
R82	`$FWDIR/lib/gtp.def`
R81.20	`/opt/CPR8120CMP-R82/lib/gtp.def`
R81.10	`/opt/CPR8120CMP-R82/lib/gtp.def`
Quantum Spark Appliance 1500 / 1600 / 1800上のR81.10.x	`/opt/CPSFWR81CMP-R82/lib/gtp.def`
R81	`/opt/CPR8120CMP-R82/lib/gtp.def`
R80.40	`/opt/CPR8040CMP-R82/lib/gtp.def`
MaestroのR80.30SP	`/opt/CPR8040CMP-R82/lib/gtp.def`
R80.30	`/opt/CPR8040CMP-R82/lib/gtp.def`
MaestroのR80.20SPまたはスケーラブルシャーシ	`/opt/CPR8040CMP-R82/lib/gtp.def`
R80.20	`/opt/CPR8040CMP-R82/lib/gtp.def`

対象セキュリティゲートウェイのバージョン	ファイルの場所
Quantum Sparkアプライアンス1500 / 1600 / 1800のR80.20.x	`/opt/CPSFWR80CMP-R82/lib/gtp.def`
R80.10	`/opt/CPR8040CMP-R82/lib/gtp.def`
SMBアプライアンス1100 / 1200R / 1400上のR77.20.x	`/opt/CPSFWR77CMP-R82/lib/gtp.def`

Health Check Point Tool

HealthCheck Point(HCP) ツールは、自己更新可能なツール群 :

- **テスト** : システムの健全性を評価します。
- **WTS(What's The Story)** : システムで発生した重要で有益な出来事の年表を提供します。
- **トポロジ** : ファイアウォールのトポロジを可視化します。

HCPツールは、管理下のセキュリティゲートウェイで6時間ごとに実行され、Security Management Server/Domain Management Serverにステータスレポートを送信します。

SmartConsoleのHCPステータスレポートは、デフォルトではすべての管理対象デバイスで**無効になっています**。

HCPステータスレポートが有効な場合、SmartConsoleはシステム全体のステータスの一部としてHCPステータスレポートを表示します。

HCPツールの詳細については[sk171436]を参照してください。

すべての管理対象デバイスのHCPツールステータスレポートを有効にするには

1. Gateways & Serversビューに移動し、上部のツールバーから**Actions**をクリックします。
2. ドロップダウンメニューから、**Enable HealthCheck Point Alerts**を選択します。

すべての管理対象デバイスの HCP ツールステータスレポートを無効にするには

1. Gateways & Serversビューに移動し、上部のツールバーの**Actions**をクリックします。
2. ドロップダウンメニューから、**Disable HealthCheck Point Alerts**を選択します。

特定の管理対象デバイスの HCP ツールステータスレポートを有効にするには

1. **Gateways & Servers**ビューに移動します。
2. 管理対象デバイスオブジェクトを右クリックします。
3. ドロップダウンメニューから**Actions**を選択し、**Enable HealthCheck Point Alerts**を選択します。

特定の管理対象デバイスのHCPツールステータスレポートを無効にするには

1. **Gateways & Servers**ビューに移動します。
2. 管理対象デバイスオブジェクトを右クリックします。
3. ドロップダウンメニューから**Actions**を選択し、**Disable HealthCheck Point Alerts**を選択します。

特定のレガシーVSXゲートウェイ/レガシーVSXクラスタに対して、HCPツールによるステータスレポートを有効にするには、以下の手順に従います。

1. SmartConsoleのウィンドウをすべて閉じます。
2. 接続*Database Tool (GuiDBEdit Tool)*Security Management Server/Domain Management Serverに追加します。
3. 左上のパネルで、**Table** > **Network Objects**と進み、**network_objects**をクリックします。
4. 右上のパネルで、レガシーVSXゲートウェイ / レガシーVSXクラスタオブジェクトをクリックします。
5. 下のパネルで、属性 **"hcp"** を右クリック > **"Edit"** をクリック > 値を **"true"** に変更 >**OK** をクリックします。
6. 変更を保存します: **File**メニュー > **Save All**をクリックします。
7. データベースツール(GuiDBEditツール) を閉じます。

特定のレガシーVSX ゲートウェイ/レガシーVSXクラスタに対して、HCP ツールによるステータスレポートを無効にする手順

1. SmartConsoleのウィンドウをすべて閉じます。
2. 接続*Database Tool (GuiDBEdit Tool)*をSecurity Management Server/Domain Management Serverに追加します。
3. 左上のパネルで、**Table** > **Network Objects**と進み、**network_objects**をクリックします。
4. 右上のパネルで、レガシーVSXゲートウェイ / レガシーVSXクラスタオブジェクトをクリックします。
5. 下のパネルで、属性 **"hcp"** を右クリック > **"Edit"** をクリック > 値を **"false"** に変更 >**OK**をクリックします。
6. 変更を保存します: **File** メニュー > **Save All**をクリックします。
7. データベースツール(GuiDBEditツール) を閉じます。

SmartConsoleのステータス

SmartConsoleは、Gateways & Serversビューにこれらのステータスを表示します:

- - 成功
- - 警告
- - エラー
- - ステータスの報告なし

ベストプラクティス - sk171436の説明に従って、SmartConsoleにHCPエクステンションをインストールします。"Warning"または "Error "ステータスを解決するには、**HealthCheck Point** ビューで **"Gateways & Servers"**ボタンをクリックし、HCPレポートを参照してください。

SmartConsoleでHCPのステータスを確認するには

1. [ゲートウェイ & サーバ] ビューで、 [セキュリティゲートウェイ] オブジェクトを右クリックします。
2. ドロップダウンメニューから、**Monitor**を選択します。
3. 開いたウィンドウで、**Device Status**へアクセスします。
4. **HealthCheck Point**セクションにスクロールダウンします。

   ここでは、簡単な説明と詳細な説明の両方を含むステータスを表示できます。

   注 - Gateways & Serversビューで:
   - HCPステータスの簡単な説明については、セキュリティゲートウェイの**Status**カラムにカーソルを合わせてください。
   - HCPステータスの詳細については、特定のセキュリティゲートウェイを選択し、画面下部の**Alerts**タブを参照してください。

制限事項

- 従来のVSX仮想システムのステータスは、仮想システムオブジェクト自体には表示されません。

  代わりに、親となるレガシーVSXゲートウェイ / レガシーVSXクラスタオブジェクトに表示されます。

- スケーラブルプラットフォーム(ElasticXL、Maestro、Scalable Chassis) を表すSMOセキュリティゲートウェイオブジェクトの場合、HealthCheck Point のステータスはセキュリティグループ全体の集約ステータスです(各セキュリティグループメンバの個別ステータスではありません) 。

オブジェクトの管理

ネットワークオブジェクトはSmartConsoleで定義され、Check Point独自のオブジェクトデータベースに格納されます。物理および仮想ネットワークコンポーネント(セキュリティゲートウェイ、サーバ、ユーザなど)、論理コンポーネント(IPアドレスレンジ、ダイナミックオブジェクトなど)を表します。これらのコンポーネントはそれぞれ、Check Pointのセキュリティ管理構成におけるオブジェクトに対応しています。Networkオブジェクトを作成する前に、組織のニーズを分析してください。

- ネットワークの物理コンポーネント(デバイス、ホスト、セキュリティゲートウェイ、およびそれらのアクティブなSoftware Blade)は何なのか。
- 論理コンポーネントは何なのか(サービス、リソース、アプリケーション、レンジなど)。
- ユーザは誰なのか。グループ化の仕方、権限の与え方をどうするか。

注 - SmartConsoleでは、オブジェクトのプロパティを設定し、元のオブジェクトから新しいオブジェクトを作成した場合、新しいオブジェクトは元のオブジェクトエディタでは使用できません。

この問題を解決するには:

1. 2つ目のObject Editorを閉じた後、元のObject EditorでOKをクリックします。
2. 元のオブジェクトを再度編集します。これで新しいオブジェクトが利用可能になります。

オブジェクトのカテゴリ

SmartConsoleのオブジェクトは、ネットワーク、デバイス、プロトコル、リソースを表します。
SmartConsoleでは、オブジェクトを次のカテゴリに分類しています。

アイコン	オブジェクトタイプ	例
	ネットワーク・オブジェクト	セキュリティゲートウェイ、ホスト、ネットワーク、アドレス範囲、動的オブジェクト、セキュリティゾーン
	サービス	サービス、サービスグループ
	カスタムアプリケーション/サイト	アプリケーション、カテゴリ、モバイルアプリケーション
	VPNコミュニティ	サイト間またはリモートアクセスコミュニティ
	ユーザ	ユーザ、ユーザグループ、ユーザテンプレート
	データタイプ	国際銀行口座番号 - IBAN、HIPAA - 医療記録番号 - MRN、ソースコード。
	サーバ	信頼できる認証局、RADIUS、TACACS
	時間オブジェクト	時間、時間グループ
	UserCheckインタラクション	メッセージウィンドウ**Ask**、**Cancel**、**Certificate Template**、**Inform**、**Drop**
	制限	ダウンロードとアップロードの帯域幅 **重要：** ポリシーのインストール後、これらのシナリオのいずれかでアクション"**Limit**"を持つアクセスコントロールルールに一致する接続に帯域幅の制限が適用されません。 ■ セキュリティオブジェクトで'**Keep all connections**'オプションが選択されています。 ■ このルールで使用されるサービスオブジェクトでは、'**Keep connections open after the policy has been installed**'オプションが選択されています。

オブジェクトを使ったアクション

オブジェクトの追加、編集、削除、クローンが可能です。クローンとは、異なる名前を持つ元のオブジェクトのコピーです。また、ポリシーの中のあるオブジェクトを別のオブジェクトに置き換えることもできます。

注 - 同じ名前のオブジェクトを2つ作らないでください。SmartConsoleのセッションを公開しようとすると、検証エラーが表示されます。解決するには、オブジェクト名を変更します。

オブジェクトを操作するには、オブジェクトツリーまたはオブジェクトエクスプローラーでオブジェクトを右クリックし、アクションを選択します。

使用されていないオブジェクトを削除したり、オブジェクトが使用されている場所を調べたりすることができます。

オブジェクトのクローンを作成するには

1. オブジェクトツリーまたはオブジェクトエクスプローラで、オブジェクトを右クリックし、**Clone**を選択します。

   Clone Objectウィンドウが開きます。

2. クローンオブジェクトの名前を入力します。
3. クリック**OK**。

オブジェクトが使用されている場所を調べるには

オブジェクトツリーまたはオブジェクトエクスプローラで、オブジェクトを右クリックし、**Where Used**を選択します。

オブジェクトを別のオブジェクトに置き換えるには

1. オブジェクトツリーまたはオブジェクトエクスプローラで、オブジェクトを右クリックし、**Where Used**を選択します。
2. **Replace**のアイコンをクリックします。
3. **Replace with**リストから、項目を選択します。
4. **Replace**をクリックします。

オブジェクトのすべてのインスタンスを削除するには

1. オブジェクトツリーまたはオブジェクトエクスプローラで、オブジェクトを右クリックし、**Where Used**を選択します。
2. **Replace**のアイコンをクリックします。

3. **Replace with**リストから、**None (remove item)**を選択します。
4. **Replace**をクリックします。

注

- 他の既存のオブジェクト(**"オブジェクト1"**)のエディタから新しいオブジェクト(**"オブジェクト2"**)を作成した場合、オブジェクト2はオブジェクト1のエディタにすぐには表示されないことがあります。オブジェクト1のエディタにオブジェクト2を表示するには、**OK**をクリックしてオブジェクト1を閉じ、再度開きます。
- SmartConsoleでは、2文字以上の名前を持つオブジェクトのみを検索またはフィルタリングできます。

オブジェクト タグ

オブジェクト タグとは、ネット ワークオブジェクト やオブジェクト のグループに検 索 用 に割り当 てるキー ワード やラベルのことです。割り当 てられるタグのタイプは次 のとおりです。

- ユーザタグ - 個 々 のオブジェクト やオブジェクト のグループに対して手 動 で割り当 てられます。
- システムタグ - "アプリケーション "など、事 前 に定 義 されたキーワード 。

各 タグには名 前 と値 があります。この値 は静 的 にすることも、検 出 エンジンによって動 的 に入 力 することもできます。

オブジェクト へのタグの追 加

オブジェクト にタグを追 加 するには

1. 編 集 するネット ワーク オブジェクト を開きます。
2. **Add Tag**フィールド に、このオブジェクト に関 連 付 けるラベルを入 力 します。
3. **Enter**を押 します。

   新 しいタグは、**Add Tag**フィールド の右 側 に表 示 されます。
4. クリック**OK**。

ネットワークオブジェクトの種類

ここでは、SmartConsoleで利用できる様々なオブジェクトタイプを説明します。

ネットワーク

ネットワークは、ネットワークアドレスとネットマスクで定義されるIPアドレスのグループです。ネットマスクは、ネットワークの大きさを示します。

ブロードキャストIPアドレスは、指定されたネットワーク上のすべてのホストを宛先とするIPアドレスです。このアドレスが含まれている場合、ブロードキャストIPアドレスはネットワークの一部とみなされます。

ネットワークグループ

ネットワークグループは、ホスト、ゲートウェイ、ネットワーク、その他のグループの集合体です。グループは、ネットワーク管理を容易かつ簡素化するために使用できます。ルールベース内の異なる場所で使用する同じオブジェクトのセットがある場合、そのオブジェクトのセットを含むグループを作成し、再利用することができます。変更は、グループの各メンバーではなく、グループに対して反映されます。

また、1つのオブジェクトしか選択できないSmartConsoleで、複数のオブジェクトを操作する必要がある場合、グループを使用します。例えば、セキュリティゲートウェイオブジェクト > **Network Management** > **VPN Domain** > **Manually defined**では、ドロップダウンメニューからオブジェクトのみを選択できます。VPNドメインに複数のオブジェクトを選択する場合は、グループを作成し、必要なオブジェクトをグループに追加し、ドロップダウンメニューからグループを選択します。

ネットワークオブジェクトのグループ化

ネットワークオブジェクトのグループを作成するには

1. **Objects**ツリーで、**New** > **Network Group**をクリックします。

   New Network Groupウィンドウが開きます。
2. グループの名前を入力します。
3. 以下のオプションのパラメータを設定します。
   - オブジェクトコメント
   - カラー
   - タグ(カスタム検索条件として)
4. 追加する各ネットワークオブジェクトについて、[+]記号をクリックし、表示されるリストから選択します。
5. クリック**OK**。

バージョンR80.20.M2以降では、オブジェクトエディタから直接ネットワークオブジェクトにグループを関連付けることもできるようになりました。

ネットワークオブジェクトにグループを関連付けるには

1. オブジェクトエディタを開き、ナビゲーションツリーの**Groups**を開きます。
2. 追加するグループごとに [+] 記号をクリックし、表示されたリストから選択します。

Check Pointホスト

Check Pointホストは複数のインタフェースを持つことができますが、ルーティングは行われません。これは、そのインタフェースを通じて自分自身のためにトラフィックを受信するエンドポイントです。(これに対して、セキュリティゲートウェイは複数のインタフェース間でトラフィックをルーティングします) 。例えば、接続されていない2つのネットワークでSecurity Management Serverとログサーバを共有する場合、共通のサーバをCheck Point Hostオブジェクトとして構成します。

Check Pointホストには、1つまたは複数のSoftware Bladeがインストールされています。ただし、Check PointホストでFirewall Bladeが有効になっている場合は、Check Pointホストをセキュリティゲートウェイとして機能させることはできません。ホストには、実際のセキュリティゲートウェイが提供するSICやその他の機能が必要です。

Check Pointホストにはルーティングメカニズムがなく、IP転送もできないため、アンチスプーフィングを実装することはできません。これらのいずれかを実行する必要がある場合は、ホストをSecurity Gatewayに変換します。

Security Management Serverオブジェクトは、Check Pointホストです。

注 - R77.30 以前のバージョンから管理サーバをアップグレードすると、ノードオブジェクトはホストオブジェクトに変換されます。

ゲート ウェイ クラスタ

クラスタは、1つの論 理オブジェクトとして構 成されたセキュリティゲート ウェイのグループです。クラスタ化 されたゲート ウェイは、ハイアベイラビリティや負 荷 分 散により冗 長 性を確 保します。

詳 細は次を参 照: *R82 ClusterXL Administration Guide*。

アドレス範囲

アドレス範囲とは、ネットワーク上のIPアドレスの範囲のことで、最小のIPアドレスと最大のIPアドレスで定義されます。ネットワークIPとネットマスクでIPアドレスの範囲を定義できない場合は、アドレス範囲オブジェクトを使用します。Address Rangeオブジェクトは、NATやVPNを実装する際にも必要です。

ワイルドカードオブジェクト

ワイルドカードオブジェクトは、セキュリティポリシーでアクセスを許可または拒否することができる共通のパターンを持つIPアドレスオブジェクトです。

注 - この機能は、Security Gateway R80.20以降でのみサポートされています。

新しいワイルドカードオブジェクトを作成するには

1. **Object Explorer** >**New** >**More** >**Network Object** >**Wildcard object**を開きます。
2. ワイルドカードIPアドレスとワイルドカードネットマスクをIPv4またはIPv6形式で入力します。
3. クリック**OK**。

ワイルドカードオブジェクトについて

ワイルドカードオブジェクトには、ワイルドカードIPアドレスとワイルドカードネットマスクが含まれます。

*ワイルドカードネットマスク*は、IPアドレスのどの部分が一致し、どの部分が一致しなくてもよいかを示すビットのマスクです。例：

ワイルドカードIP:	194.	29.	0.	1
ワイルドカードネットマスク:	0.	0.	3.	0

第3オクテットは、ビットのマスクを表します。3を2進数に変換すると、00000011となります。

マスクの0の部分は、IPアドレスの相当するビットと一致させる必要があります。

マスクの1の部分は一致する必要はなく、任意の値にできます。

0 0 0 0 0 0 IPアドレスの同等ビットと一致しなければならない	1 1 一致させる必要はない

2進数のネットマスクで、次のような10進数値を生成します。

128	64	32	16	8	4	2	1	
						バイナリ		**10進数**
0	0	0	0	0	0	0	0	**0**
0	0	0	0	0	0	0	1	**1**
0	0	0	0	0	0	1	0	**2**
0	0	0	0	0	0	1	1	**3**

ネットマスクは、これらのIPアドレスのみを許可します。

- 194.29.0.1
- 194.29.1.1
- 192.29.2.1
- 194.29.3.1

使用例

シナリオ1

あるスーパーマーケットチェーンでは、すべてのレジがサブネット194.29.x.1(xは地域を定義) にあります。この使用例では、この地域のすべてのレジが194.30.1.1のデータベースサーバにアクセスする必要があります。

256のホスト(194.29.0.1, 194.29.1.1, 194.29.2.1...194.29.255.1) を定義する代わりに、管理者は地域内のすべてのレジを示すワイルドカードオブジェクトを作成します。

ワイルドカードIP:	194.	29.	0.	1
ワイルドカードのマスク:	0.	0.	255.	0

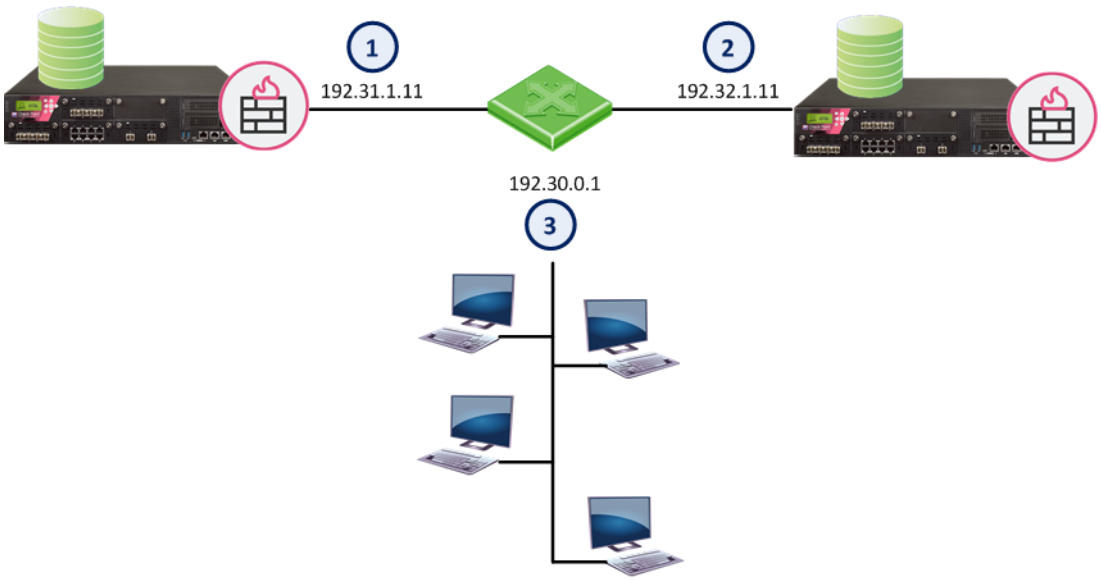
これで、ワイルドカードオブジェクトをアクセスコントロールポリシーに追加できるようになりました。

発信元	宛先	アクション	追跡
ワイルドカードオブジェクト	データベースサーバオブジェクト	承認	ログ記録

シナリオ2

この使用例では、ヨーロッパとアジアに店舗を持つスーパーマーケットチェーンを考えます。

192.30.0-255.1ネットワークには、アジア地域とヨーロッパ地域、およびそれらの地域内の店舗が含まれています。



項目	説明
1	欧州向けデータベースサーバ
2	アジア向けデータベースサーバ
3	欧州、アジアネットワーク

管理者は、ヨーロッパ地域とアジア地域の店舗が異なるデータベースサーバにアクセスすることを望んでいます。このトポロジでは、ヨーロッパとアジアのネットワークのIPアドレスの第3オクテットは、ワイルドカードの対象となります。ワイルドカードの最初の4ビットが地域を表し、最後の4ビットが店舗番号を表します。

地域を表すビット	店番号を表すビット
0000	0000

ワイルドカード IP:

- アジア地域は**0001xxxx**(10進数でリージョン**1**) で表されます。
- 欧州地域は**0010xxxx**(10進数でリージョン**2**) で表されます。

バイナリ:

バイナリ		10進数
地域	ストア	
0001	0000	16 - アジア地域
0010	0000	32 - 欧州地域

特定の地域のすべての店舗を含めるには、ワイルドカードマスクの最後の4ビットを1(10進数で15) に設定する必要があります。

バイナリ		**10進数**
地域	**ストア**	
xxxx	1111	15 - アジア全店舗
xxxx	1111	15 - ヨーロッパ全店舗

アジアのすべての店舗を表すワイルドカードオブジェクトは、次のようになります。

ワイルドカードIPアドレス	192.30.16.1	(地域)
ワイルドカードネットマスク	0.0.15.0	(地域内店舗向け)

この範囲のIPアドレスの場合192.30.**16-31**.1

ヨーロッパのすべての店舗を表すワイルドカードオブジェクトは、次のようになります。

ワイルドカードIPアドレス	192.30.32.1	(地域)
ワイルドカードネットマスク	0.0.15.0	(地域内店舗向け)

この範囲のIPアドレスの場合192.30.**32-47**.1

管理者は、アクセスコントロールポリシーでこれらのワイルドカードオブジェクトを使用できるようになりました。

発信元	**宛先**	**アクション**	**追跡**
アジア店舗のワイルドカード	アジア向けデータベースサーバ	承認	ログ記録
ヨーロッパ店舗のワイルドカード	欧州向けデータベースサーバ	承認	ログ記録

シナリオ3

このシナリオでは、ネットマスクビットは連続していません。

ワイルドカード IP	1	1	0	1
ワイルドカードマスク	0	0	5	0

ワイルドカード IP	00000001.00000001.00000000.00000001
ワイルドカードマスク	00000000.00000000.00000101.00000000

マスク:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0

これらのIPアドレスにのみマッチします。

IP アドレス	バイナリ	コメント
1.1.0.1	00000001.00000001.00000000.00000001	IPアドレス
1.1.1.1	00000001.00000001.00000001.00000001	位置23の等価ビットは重要ではありません
1.1.4.1	00000001.00000001.00000100.00000001	位置21の等価ビットは重要ではありません
1.1.5.1	00000001.00000001.00000101.00000001	21と23の位置の等価ビットは重要ではありません

IPv6

IPv6アドレスにも同じ原則が適用されます。例えば、ワイルドカードオブジェクトが以下の値を持つ場合を考えます。

IPv6アドレス	2001::1:10:0:1:41
ワイルドカードネットマスク	0::ff:0:0

ワイルドカードは、2001::1:10:0-255:1:41にマッチ

ドメイン

Domainオブジェクトは、ホストまたはDNSドメインをその名前だけで表します。サイトのIPアドレスは必要ありません。

ドメインオブジェクトは、アクセスコントロールポリシーの送信元と送信先のカラムで使用することができます。

Domainオブジェクトは2つの方法で設定することができます。

- 選択**FQDN**

  オブジェクト名には、FQDN(Fully Qualified Domain Name: 完全修飾ドメイン名) を使用します。

  .x.y.z (FQDNの前にドット ". "を付ける) の形式で使用します。

  例えば、.www.example.comを使用した場合、セキュリティゲートウェイは以下のようにマッチします。www.example.com

  このオプションは、R80.10以降でサポートされ、デフォルトとなっています。非FQDNオプションよりも正確で高速です。

  セキュリティゲートウェイはダイレクトDNSクエリでFQDNを検索し、その結果をルールベースで使用します。

  このオプションは、SecureXL Acceptテンプレートに対応しています。

  ルール内でこのオプションを使用してドメインオブジェクトを使用しても、ルールやその後に続くルールのパフォーマンスには影響ありません。

- クリア**FQDN**

  このオプションは、ドメインとそのサブドメインを強制するものです。

  オブジェクト名には、.x.yの形式を使用します。

  例えば、名前に.example.com または.example.co.ukを使用します。

  example.comを使用した場合、セキュリティゲートウェイはwww.example.comと一致します。support.example.com

  セキュリティゲートウェイはDNSの逆引きを使って名前を解決しますが、不正確な場合があります。

  セキュリティゲートウェイはルールベースの結果を使用し、再度使用するために結果をキャッシュします。

更新可能なオブジェクト

更新可能オブジェクトについて

Updatable Objectは、Office 365、AWS、GEOロケーションなどの外部サービスを表すネットワークオブジェクトです。外部サービスプロバイダは、そのサービスへのアクセスを許可するために、IPアドレスまたはドメイン、あるいはその両方のリストを公開しています。これらのリストは動的に更新されます。

更新可能オブジェクトは、Check PointがCheck Pointクラウドにアップロードするプロバイダの公開リストからその内容を取得します。更新可能なオブジェクトは、プロバイダがリストを変更するたびに、Security Gateway上で自動的に更新されます。アップデートを有効にするために、ポリシーをインストールする必要はありません。

更新可能オブジェクトは、3種類のポリシー(アクセスコントロール、脅威対策、HTTPSインスペクション)すべてで使用できます。

アクセスコントロール、Threat Prevention、またはHTTPSインスペクションポリシーの更新可能なオブジェクトをソースまたは宛先として使用することができます。Threat Preventionポリシーでは、更新可能なオブジェクトを保護スコープとして使用することもできます。

注:

- アクセスコントロールについては、Security Gateway R80.20以降でサポートされます。
- 脅威対策とHTTPSインスペクションについては、Security Gateway R80.40以降でサポートされる機能です。
- 更新可能オブジェクトをネットワークグループに追加することはできません。

アクセスコントロールポリシーへの更新可能オブジェクトの追加

1. Security Management Server/Domain Management Serverとセキュリティゲートウェイが、インターネット上のCheck Pointクラウドにアクセスできることを確認します(sk83520を参照)。
2. SmartConsoleでSecurity Management Server/Domain Management Serverにアクセスします。
3. 左側のナビゲーションパネルで**Security Policies**をクリックします。
4. 上部パネルで、**Access Control** > **Policy**をクリックします。
5. 必要な位置に新しいルールを追加します。
6. **Destination**カラムで、**+**アイコンをクリックします。

   注 - 更新されたオブジェクトは、**Source**カラムに追加することもできます。

7. 右上の隅で、**Import** >**Updatable Objects** をクリックします。

   Updatable Objectsウィンドウが開きます。

8. 追加する更新可能オブジェクトを選択します。
9. クリックOK。

   選択された更新可能オブジェクトがルールカラムに追加されます。
10. このルールで他のカラムを設定します。
11. SmartConsoleセッションを公開する。
12. アクセスコントロールポリシーをインストールします。

カスタム脅威対策ポリシーへの更新可能オブジェクトの追加

1. Security Management Server/Domain Management Serverとセキュリティゲートウェイが、インターネット上のCheck Pointクラウドにアクセスできることを確認します(sk83520を参照) 。
2. SmartConsoleでSecurity Management Server/Domain Management Serverにアクセスします。
3. 左側のナビゲーションパネルで**Security Policies**をクリックします。
4. 上部パネルで、**Threat Prevention** > **Custom Policy**をクリックします。
5. 必要な位置に新しいルールを追加します。
6. **Protected Scope**カラムで、**+**アイコンをクリックします。
7. 右上の隅で、**Import** > **Updatable Objects**をクリックします。

   Updatable Objectsウィンドウが開きます。

   注 - Sourceカラムにオブジェクトを追加することもできます。
8. 追加する更新可能オブジェクトを選択します。
9. クリックOK。

   選択された更新可能オブジェクトがルールカラムに追加されます。
10. このルールで他のカラムを設定します。
11. SmartConsoleセッションを公開する。
12. 脅威対策ポリシーをインストールします。

HTTPSインスペクションポリシーへの更新可能オブジェクトの追加

1. Security Management Server/Domain Management Serverとセキュリティゲートウェイが、インターネット上のCheck Pointクラウドにアクセスできることを確認します(sk83520を参照) 。
2. SmartConsoleでSecurity Management Server/Domain Management Serverにアクセスします。
3. 左側のナビゲーションパネルで**Security Policies**をクリックします。
4. 上部パネルで、該当するポリシーをクリックします:
   - **HTTPS Inspection>Inbound Policy**
   - **HTTPS Inspection>Outbound Policy**
5. 必要な位置に新しいルールを追加します。
6. **Destination**カラムで、**+**アイコンをクリックします。

   注 - 更新されたオブジェクトは、**Source**カラムに追加することもできます。

7. 右上の隅で、**Import > Updatable Objects**をクリックします。

   Updatable Objectsウィンドウが開きます。
8. 追加する更新可能オブジェクトを選択します。
9. クリック**OK**。

   選択された更新可能オブジェクトがルールカラムに追加されます。
10. このルールで他のカラムを設定します。
11. SmartConsoleセッションを公開する。
12. HTTPS インスペクションポリシーをインストールします。

更新可能オブジェクトのモニタリング

更新可能オブジェクトが対応するIPアドレスをどのように更新するかは、SmartConsoleまたはSmartViewのLogs & Events > Logsタブでモニタできます。

最も適した手順に従います。

手順 1 - ポリシーから選択した更新可能オブジェクトのすべてのログを表示する

1. 左側のナビゲーションパネルでSecurity Policiesをクリックします。
2. 上部パネルで、該当するポリシーをクリックします:
   - Access Control>Policy
   - Threat Prevention>Custom Policy
3. 該当するUpdatedオブジェクトを含むルールを探します。
4. 更新されたオブジェクトにマウスカーソルを合わせます。
5. 表示されたメニューで、Show Logsアイコン(クリップボードのアイコン) をクリックします。

   Logsウィンドウが開き、一番上の検索フィールドに二重引用符で囲まれた更新可能コンテナの名前が表示されます。
6. 左側で、該当する期間を選択します。
7. 該当するログエントリをダブルクリックします。

   Log Detailsウィンドウが開きます。
8. アップデートが成功すると、Statusフィールドが表示されます:

   ```
   Succeeded
   ```

手順 2 - ログから特定の更新可能オブジェクトを検索する

1. 左のナビゲーションパネルから、Logs & Events > Logsをクリックします。
2. 上部の検索バーに、更新可能オブジェクトの名前を二重引用符で囲んで入力します。

   例:

   ```
   "Office365 Services"
   ```
3. 左側で、該当する期間を選択します。
4. 該当するログエントリをダブルクリックします。

   Log Detailsウィンドウが開きます。
5. アップデートが成功すると、Statusフィールドが表示されます:

   ```
   Succeeded
   ```

管理サーバによる更新可能オブジェクトの更新

セキュリティゲートウェイがインターネットに接続されていない場合、管理サーバ(プロキシサーバとして機能)を介して更新可能オブジェクトの更新を取得できます:

1. セキュリティゲートウェイ/各クラスタメンバ/Scalable Platformセキュリティグループのコマンドラインに接続します。
2. エキスパートモードにログインします。
3. 現在の設定ファイルをバックアップします:

```
cp -v $CPDIR/conf/downloads/dl_prof_ONLINE_SERVICES.xml{,_
BKP}
```

4. 現在の設定ファイルを編集します:

```
vi $CPDIR/conf/downloads/dl_prof_ONLINE_SERVICES.xml
```

5. "ProxyRoute" パラメータの値を0から1に変更します:

```
<ProxyRoute>1</ProxyRoute>
```

例(ファイルの下部を参照):

```
<?xml version="1.0" encoding="UTF-8"?>
<DownloadPreferences>
    <ModuleName>Online_Services</ModuleName>
    <ID>111</ID>
    <Version>1.0</Version>
    <Files>online_services_gw.tgz</Files>
    <DeletionMethod>2</DeletionMethod>
    <Interval>120</Interval>
    <SVT_Log_ID>Firewall</SVT_Log_ID>
    <SVT_Log_Desc>IPs and Domains for Online Services
objects</SVT_Log_Desc>
    <SVT_Log_Severity>2</SVT_Log_Severity>
    <SVT_Log_Failure_Impact>Online Services objects update has
failed</SVT_Log_Failure_Impact>
    <CK_Identifier>fw1:6.0:xlate</CK_Identifier>
    <CK_Identifier>fw1:6.0:auth</CK_Identifier>
    <CK_Identifier>fw1:6.0:content</CK_Identifier>
    <URL>
https://updates.checkpoint.com/WebService/services/DownloadMetaDa
taService?wsdl</URL>
    <Updatable>Yes</Updatable>
    <ProxyRoute>1</ProxyRoute>
</DownloadPreferences>
```

6. 変更内容をファイルに保存し、エディタを終了します。
7. Scalable Platformセキュリティグループ上で、変更したファイルをすべてのセキュリティグループメンバにコピーします:

```
asg_cp2blades $CPDIR/conf/downloads/dl_prof_ONLINE_
SERVICES.xml
```

ダイナミックオブジェクト

Dynamic Objectは、セキュリティゲートウェイごとにIPアドレスが異なる「論理的」なオブジェクトで、"`dynamic_objects`"コマンドを使用して解決されます。

Security Gateway R80.10以降では、動的オブジェクトがSecureXL Acceptテンプレートに対応しています。したがって、動的オブジェクトを使用するルールや、その後に続くルールには、パフォーマンスの影響はありません。

Dynamic Objectは、**LocalMachine-all-interfaces**に事前定義されています。DAIPコンピュータインタフェース(静的および動的)は、このオブジェクトに解決されます。

一般的なデータセンターオブジェクト

R81からは、外部のWebサーバに設置されたファイルに定義されたIPアドレスへのアクセスや、外部からのアクセスを強制することができます。

そのためには、SmartConsoleの**Generic Data Center**オブジェクトを使用します。Generic Data Centerオブジェクトは、アクセスしたいIPアドレスを含む外部サーバのJSONファイルを指し示す。こうすることで、ポリシーでGeneric Data Centerオブジェクトが使用されている場合、SmartConsoleは必要に応じてJSONファイルからIP情報を取得することができます。

JSONファイルは、Security Management Server上でローカルにホストすることもできます。

この機能は、ある管理者がルールベースを作成してオブジェクトを定義し、別の管理者がそのオブジェクトの内容を管理するような場合に役立ちます。

この機能は、アクセスコントロール、Threat Prevention、HTTPSインスペクション、およびNATルールベースでサポートされています。

この機能は、Security Management Server R81以降、およびSecurity Gateway (クラスタ) R81以降でのみサポートされています。

Generic Data Centerオブジェクトを作成した後、ファイルに加えられた変更は、ポリシーをインストールする必要なく、自動的にSecurity Gatewayに適用されます。

JSONファイルを作成するには、sk167210に記載されているガイドラインに従ってください。

セキュリティポリシーでの汎用データセンターオブジェクトの使用

1. SmartConsole のオブジェクトエクスプローラーで、**New** >**More** >**Cloud** >**Data Center** >**Generic Data Center** をクリックします。

   New Generic Data Centerオブジェクトウィンドウが開きます。

2. 次のフィールドを設定します。

   a. **URL**- JSONファイルのURLを入力します。

   b. **Interval**- ファイルがサンプリングされる内部を入力します。

      デフォルトの間隔は60秒です。

   c. **Add Custom Header**- サーバへのリクエストにカスタムヘッダを追加する必要がある場合は、このチェックボックスを選択し、**Key** と**Value**を入力します。

   d. **Test Connection**をクリックして、ファイルにアクセスできることを確認します。

3. 該当する汎用データセンターオブジェクトをルールベースに追加します。

   Sourceまたは**Destination**カラムで、**Import** >**Data Center** >**Generic Data Center** をクリックし、リストから該当するデータセンターオブジェクトを選択します。

   注 - リストには、JSONファイルに含まれるすべてのデータセンターオブジェクトが含まれます。

4. **Install Policy**。

制限事項

- JSONファイルがサンプリングされる2つの時間間隔の間に、JSONファイルに最大15,000の変更を加えることができます。
- セキュリティゲートウェイは、次のタイプのオブジェクトを合計5,000個サポートします：動的オブジェクト、更新可能オブジェクト、汎用データセンターオブジェクト、ネットワークフィードオブジェクト。

セキュリティゾーン

セキュリティゾーンを使用すると、ネットワークの部分間のトラフィックを制御する強力なアクセスコントロールポリシーを作成することができます。

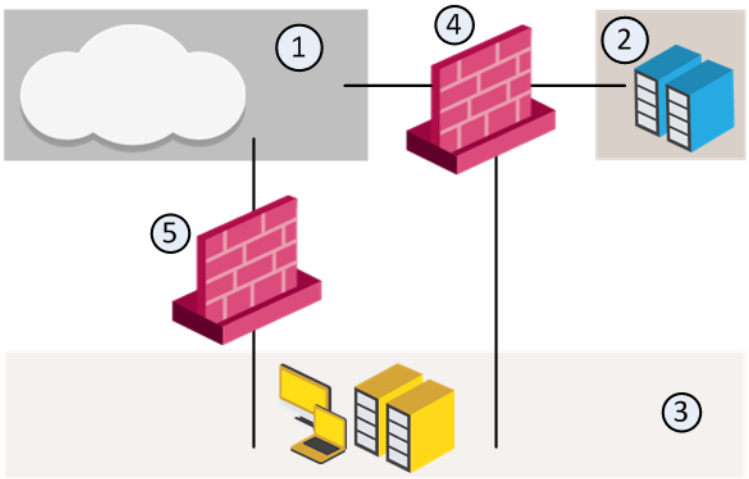
セキュリティゾーンオブジェクトは、ネットワークの一部(例えば、内部ネットワークや外部ネットワーク)を表します。セキュリティゲートウェイのネットワークインタフェースをセキュリティゾーンに割り当てます。そして、ルールベースのSourceカラムとDestinationカラムで、Security Zoneオブジェクトを使用することができます。

セキュリティゾーンは、次の目的で利用します。

- ポリシーの簡素化 多くのセキュリティゲートウェイに同じルールを適用する。
- ルールベースを変更することなくセキュリティゲートウェイのインタフェースにネットワークを追加する。

例えば、この図では典型的なネットワークに3つのセキュリティゾーン(*ExternalZone*(1)、*DMZZone*(2)、*InternalZone*(3)) があります。

- セキュリティゲートウェイ (4) は3つのインタフェースを持つ。1つのインタフェースが*ExternalZone*(1) に、1つのインタフェースが*DMZZone*(2) に、1つのインタフェースが*InternalZone*(3) に割り当てられています。
- セキュリティゲートウェイ(5)は2つのインタフェースを持つ。1つのインタフェースが*ExternalZone*(1) に、1つのインタフェースが*InternalZone*(3) に割り当てられています。



セキュリティゲートウェイインタフェースは、1つのセキュリティゾーンにのみ属することができます。異なるネットワークへのインタフェースは、同じセキュリティゾーンに置くことができます。

ワークフロー

1. セキュリティゾーンのオブジェクトを設定します。

   または、定義済みのセキュリティーゾーン (*事前定義されたセキュリティゾーン (306ページ)*)。

2. セキュリティゲートウェイのインタフェースをセキュリティゾーンに割り当てます。*セキュリティゾーンの作成と割り当て (305ページ)*)。
3. ルールのSourceとDestinationにSecurity Zoneオブジェクトを使用します。

   例:

発信元	宛先	VPN	サービス	アクション
InternalZone	ExternalZone	任意のトラフィック	Any	承認

4. アクセスコントロールポリシーをインストールします(*アクセスコントロールポリシーのインストール (395ページ)*)。

セキュリティゾーンとNATルール使用時のルールベース実行処理のフロー

1. **NATルールのマッチング**

   システムは最初のステップとして、NATルールベースマッチングを実行します。これは、変換とルーティングの両方に使用される送信IPアドレスを特定し、記録します。このステップでは、システムがトラフィックを適切なセキュリティゾーンにマッピングできるようにします。

2. **送信インタフェースの取得**

   アウトバウンドIPアドレスを特定した後、カーネルはルーティングAPIに問い合わせ、対応するネットワークインタフェースを決定します。その後、システムはこのインタフェースを適切なアウトバウンドセキュリティゾーンに割り当てます。この割り当てにより、ルールベースの実行がNATの設定と一致し、トラフィックを正確にルーティングすることが保証されます。

3. **ルールベースの実行**

   設定されたアウトバウンドインタフェースとセキュリティゾーンを使用して、システムはセキュリティポリシーを適用してトラフィックを管理します。これにより、すべてのトラフィックが事前に定義されたルールに従うことが保証され、効率的で正確なネットワーク運用がサポートされます。

例:サードパーティツールとの競合の解決

Algosecなどのサードパーティのルールベースツールでは、Check Pointのポリシーを分析する際に競合が発生することがあります。このようなコンフリクトが発生するのは、ルールベースがNAT変換IPを明示的に定義していないからです。これを解決するために、システムはメインのルールベースを実行する前に、NATルールベースを処理します。NATデータとルーティング情報を組み合わせることで、正しい発信インタフェースゾーンを設定します。この統合により、サードパーティのツールはポリシーを正しく解釈し、エラーなくトラフィックルールを実施することができます。

セキュリティゾーンの作成と割り当て

ルールベースでセキュリティゾーンを使用する前に、セキュリティゲートウェイのインタフェースをセキュリティゾーンに割り当てる必要があります。

セキュリティゾーンを作成するには

1. **Objects bar** (F11) で、**New** >**More** >**Network Object** >**Security Zone** をクリックします。

   Security Zoneウィンドウが開きます。

2. セキュリティゾーンの名前を入力します。
3. オプションでコメントやタグを入力します。
4. クリック**OK**。

インタフェースをセキュリティゾーンに割り当てるには

1. **Gateways & Servers**ビューで、Security Gatewayオブジェクトを右クリックし、**Edit**を選択します。

   Gateway Propertiesウィンドウが開きます。

2. **Network Management**ペインで、インタフェースを右クリックし、**Edit**を選択します。

   Interfaceウィンドウが開きます。**General**ペインの**Topology**エリアには、インタフェースがすでにバインドされているセキュリティゾーンが表示されます。デフォルトでは、セキュリティゾーンは、インタフェースの場所 (**Leads To**) に応じて計算されます。

3. **Modify**をクリックします。

   Topology Settingsウィンドウが開きます。

4. **Security Zone**領域で、**User Defined**をクリックし、**Specify Security Zone**を選択します。
5. ドロップダウンボックスから、セキュリティゾーンを選択します。

   または、**New**をクリックして、新規に作成します。

6. クリック**OK**。

事前定義されたセキュリティゾーン

あらかじめ定義されているセキュリティゾーンと、その目的は次のとおりです。

- **WirelessZone** - ワイヤレス接続でユーザやアプリケーションからアクセスできるネットワーク。
- **ExternalZone** - インターネットやその他の外部ネットワークなど、安全でないネットワーク。
- **DMZZone** - DMZ(非武装地帯) は、*境界*ネットワークと呼ばれることもあります。外部からアクセスできる企業のサーバが含まれます。

  DMZは、外部のユーザやアプリケーションが社内の特定のサーバにアクセスすることを許可しますが、外部のユーザが安全な社内ネットワークにアクセスすることはできません。

セキュリティゲートウェイのルールベースに、企業のDMZへのトラフィックを許可するルールを追加します。例えば、DMZにあるWebサーバへのHTTPおよびHTTPsのトラフィックを許可するルールがあります。

- **InternalZone** - 認証されたユーザのみが使用し、保護される必要がある機密データを持つ企業ネットワーク。

制限事項

- NATポリシーは、R81以降のセキュリティゲートウェイのセキュリティゾーンにのみ対応しています。
- Threat Preventionポリシーは、R81以降のセキュリティゲートウェイのセキュリティゾーンのみをサポートします。
- クリーンアップルールにセキュリティゾーンが含まれている場合、そのルールのDropテンプレートの作成が妨げられる場合があります。

外部管理のゲートウェイとホスト

外部管理のセキュリティゲートウェイまたはホストとは、Check Pointのソフトウェアがインストールされているセキュリティゲートウェイまたはホストのことを指します。

この外部管理のセキュリティゲートウェイは、外部の管理サーバによって管理されます。Check Pointのセキュリティポリシーを受け取ることはできませんが、Check PointのVPNコミュニティやソリューションに参加することができます。

相互運用可能なデバイス

相互運用可能なデバイスとは、Check Point Software Bladeがインストールされていないデバイスのことを指します。

相互運用可能なデバイスは:

- ポリシーがインストールされていない
- Check PointのVPN コミュニティやソリューションに参加可能

VoIPドメイン

VoIP Domainオブジェクトは5種類あります。

- VoIP Domain SIP Proxy
- VoIP Domain H.323 Gatekeeper
- VoIP Domain H.323 Gateway
- VoIP Domain MGCP Call Agent
- VoIP Domain SCCP Call Manager

多くのVoIPネットワークでは、制御信号はメディアとは異なるルートでネットワークを通過します。これは、通話が*信号ルーティング*デバイスによって管理されている場合です。シグナルの*ルーティング*は、SIPでは*リダイレクトサーバ*、*レジストラー*、および/または*プロキシ*によって行われます。SIPでは、信号の*ルーティング*は*ゲートキーパー*や*ゲートウェイ*によって行われます。

信号の*ルーティング*位置を実施することは、VoIPセキュリティの重要な側面です。信号ルーティングデバイスで管理できるエンドポイントを指定することが可能です。このロケーションの集合を*VoIPドメイン*と呼びます。

詳細は次を参照: *R82 VoIP Administration Guide*。

論理サーバ

論理サーバは、同じサービスを提供するマシンのグループです。このグループの作業負荷は、すべてのメンバ間で分散されます。

Servers groupフィールドにサーバグループが指定されている場合、クライアントはこの物理サーバにバインドされます。

2つの操作モードがあります。

- **Persistency by Service**- クライアントが指定されたサービスの物理サーバに接続されると、同じ論理サーバと同じサービスへのその後の接続は、セッションの間、同じ物理サーバにリダイレクトされます。
- **Persistency by Server**- クライアントが物理サーバに接続されると、同じ論理サーバへのそれ以降の接続は(どのサービスでも)、セッションの間、同じ物理サーバにリダイレクトされます。

バランス方式

負荷分散アルゴリズムは、サーバ間のトラフィックを分散する方法を定義します。バランシング方法にはいくつかの種類があります。

- **サーバ負荷** - セキュリティゲートウェイは、どのSecurity Management Serverが新しい接続を処理するのに最も適しているかを判断します。
- **ラウンドトリップ時間** - セキュリティゲートウェイとサーバ間の最短ラウンドトリップ時間(単純なpingで実行)に基づき、セキュリティゲートウェイは、新しい接続を処理するために最適なSecurity Management Serverを決定します。
- **ラウンドロビン** - 新しい接続は、最初に利用可能なサーバに割り当てられます。
- **ランダム** - 新しい接続は、ランダムにサーバに割り当てられます。
- **Domain**- 新しい接続は、ドメイン名に基づいてサーバに割り当てられます。

詳細:*R82 Quantum Security Gateway Guide*> *ConnectControlの章 - サーバのロードバランシング*。

OSE(Open Security Extension) デバイス

Open Security Extension(OSE) の機能を使用すると、サードパーティ製デバイスを Check Point SmartConsole で管理することができます。管理対象のデバイスは、ハードウェアとソフトウェアパケットの両方で、その数はライセンスに依存します。OSEデバイスには、一般的にルーティング用のハードウェアセキュリティデバイスや、専用のネットワークアドレス変換や認証アプライアンスが含まれます。セキュリティデバイスは、セキュリティポリシーの中でEmbedded Devicesとして管理されます。

Security Management Serverは、セキュリティポリシーからアクセスリストを生成し、選択したルータとオープンセキュリティデバイスにダウンロードします。Check Pointでは、次のデバイスをサポートしています。

OSEデバイス	サポートされているバージョン
Cisco Systems	9.x、10.x、11.x、12.x

Check Pointルールベースには、これらのオブジェクトを含めることはできません。もし含まれていると、Security Management Serverでアクセスリストが生成されません。

- ドロップ(Actionカラム)
- 暗号化(アクション)
- アラート(アクション)
- RPC(サービス)
- ACE(サービス)
- 認証ルール
- セルのネゲート

OSEデバイスインタフェースの定義

OSEデバイスは、起動時にネットワークインタフェースとセットアップを報告します。各OSEデバイスは、その構成をリスト表示するためのコマンドが異なります。各デバイスに少なくとも1つのインタフェースを定義する必要があります。定義しないと**ポリシーのインストール**が失敗します。

OSEデバイスを定義するには

1. オブジェクトエクスプローラーから、**New** > **More**をクリックします。
2. ネットワーク**Object** >**More** > **OSE Device**をクリックします。
3. 一般的なプロパティを入力する (*OSデバイスプロパティウィンドウ- 一般タブ (313ページ)*)。

   OSデバイスを他のサーバのホストリストに追加することも推奨します:`hosts` (Linux)と`lmhosts` (Windows)。
4. **Topology**タブを開き、デバイスのインタフェースを追加します。

デバイスの外部インタフェースでアンチスプーフィングを有効にできます。インタフェースをダブルクリックします。**Interface Properties**ウィンドウ > **Topology**タブで、**External**と**Perform Anti-Spoofing**を選択します。

5. **Setup**タブを開き、OSデバイスとその管理者認証情報を定義してください。*なりすまし防止パラメータとOSデバイスのセットアップ(Cisco) (313ページ)*)。

OSデバイスプロパティウィンドウ - 一般タブ

- **Name** - OSEデバイスの名前。ここで指定する名前は、サーバのシステムデータベースに表示されます。
- **IP Address** - デバイスのIPアドレス。
- **Get Address** - このボタンをクリックすると、名前がアドレスに解決されます。
- **Comment** - このオブジェクトが選択されたときに、**Network Object**ウィンドウの下部に表示されるテキスト。
- **Color** - ドロップダウンリストから色を選択します。SmartConsoleでは、OSEデバイスが選択した色で表示され、追跡と管理が容易になります。
- **Type** - サポートされているベンダーの一覧から選択します。

なりすまし防止パラメータとOSデバイスのセットアップ(Cisco)

Cisco(バージョン10.x以降) デバイスの場合、アンチスプーフィングパラメータから生成されるフィルタルールの方向を指定する必要があります。実施方向は、各ルータの**Setup**タブで指定します。

Ciscoルータの場合、**Spoof Rules Interface Direction**プロパティで実施方向が定義されます。

アクセスリスト番号 - 適用されているCiscoアクセスリストの数。Ciscoルータのバージョン 12x 以降では、101 ~ 200 のACL番号をサポートしています。Ciscoルータのバージョン12x以降では、101 ~ 200のACL番号範囲と、2000 ~ 2699のACL番号範囲をサポートしています。このACL番号範囲を入力することで、より多くのインタフェースをサポートできます。

各認証情報について、オプションを選択します。

- **None** - 認証情報は必要ありません。
- **Known** - 管理者が認証情報を入力する必要があります。
- **Prompt** - 管理者は認証情報の入力を求められます。

Username - OSEデバイスにログオンするために必要な名前。

Password - ルータで定義されている管理者パスワード (読み取り専用)。

Enable Username - アクセスリストのインストールに必要なユーザ名。

Enable Password - アクセスリストをインストールするために必要なパスワード。

Version - Cisco OSEデバイスのバージョン(9.x、10.x、11.x、12.x) 。

OSEデバイスインタフェース方向 - インストールされたルールは、すべてのインタフェースでこの方向に移動するデータパケットに適用されます。

Spoof Rules Interface Direction - すべてのインタフェースでこの方向に移動するデータパケットに、スプーフィング追跡ルールが適用されます。

ポリシーの管 理

SmartConsoleには、定 義 段 階とメンテナンスの両 方 において、ポリシー管 理タスクに対 応 するツールが多く備 えられています。

定 義 の段 階 :

- *ポリシーパッケージ*を使 用 すると、異 なるタイプのポリシーをグループ化して、同じインストールターゲットにまとめてインストールできます。
- *事 前 定 義 されたインストールターゲット*により、各 パッケージをゲートウェイのセットに関 連 付 けることができます。ポリシーパッケージをインストールするたびに、ゲートウェイの選 択 プロセスを繰 り返 す必 要 はありません。

メンテナンス・レベル:

- *検 索*は、ネットワークオブジェクトとルールベース内 のルールに対 する多 彩 な検 索 機 能 を提 供 します。
- *データベースのバージョン管 理*は、データベースに対 する過 去 の変 更 を追 跡 することができます。

ポリシーパッケージでの作 業

ポリシーパッケージは、さまざまな種 類 のポリシーの集 合 体 です。インストール後 、Security Gatewayはパッケージに含 まれるすべてのポリシーを実 施 します。ポリシーパッケージは、これらのポリシータイプを1つまたは複 数 持 つことができます。

- **アクセスコントロール** - 以 下 のようなタイプのルールが含 まれます。
  - ファイアウォール
  - NAT
  - アプリケーションコントロールとURLフィルタリング
  - コンテンツアウェアネス
  - モバイルアクセス
- **QoS** - 帯 域 管 理 のためのQoS(クオリティオブサービス) ルール
- **デスクトップセキュリティ** - Endpoint Security VPNリモートアクセスクライアントがスタンドアロンクライアントとしてインストールされているエンドポイントコンピュータ用 のファイアウォールポリシーです。
- **脅 威 対 策** - 次 で構 成 されています。

- IPS - IPSサービスにより継続的に更新されるIPS保護機能
- アンチボット & アドバンスドDNS - ボットに感染したマシンを検出し、ボットのコマンド & コントロール(C&C) 通信をブロックすることでボット被害を防止します。
- アンチウィルス - ヒューリスティック分析を含み、ウィルス、ワーム、その他のマルウェアをゲートウェイで阻止します。
- Threat Emulation - サンドボックス内で疑わしいファイルを開くことで、ゼロデイ攻撃や高度なポリモーフィック攻撃を検知します。
- Threat Extraction - 企業ネットワークに入る前に、Eメールの添付ファイルから潜在的に悪意のあるコンテンツを抽出します。
- ゼロフィッシング - 業界をリードする機械学習アルゴリズムと特許取得済みのインスペクション技術を活用することで、Webサイトに対する未知のゼロデイ攻撃や既知のフィッシング攻撃をリアルタイムで防止します。

■ HTTPSインスペクション - 内部のブラウザクライアントとWebサーバ間のTLS(Transport Layer Security) プロトコルによって暗号化されたトラフィックを検査するためのルールで構成されています。R82以降、HTTPSインスペクションポリシーは受信ポリシーと送信ポリシーに分けられます。

重要 -読み取り専用権限を持つ管理者がログインし、ポリシーパッケージで「デスクトップセキュリティ」ポリシーが有効になっている場合、レガシーのSmartDashboardにQoSおよびデスクトップポリシーが表示されないという問題がありました。

インストールプロセス:

■ ルールに対してヒューリスティックな検証を行い、ルールの一貫性と冗長性がないことを確認します。

検証エラーが発生した場合、ポリシーはインストールされません。検証の警告がある場合 (複数のインタフェースを持つ Security Gateway でアンチスプーフィングが有効でない場合など)、ポリシーパッケージは警告とともにインストールされます。

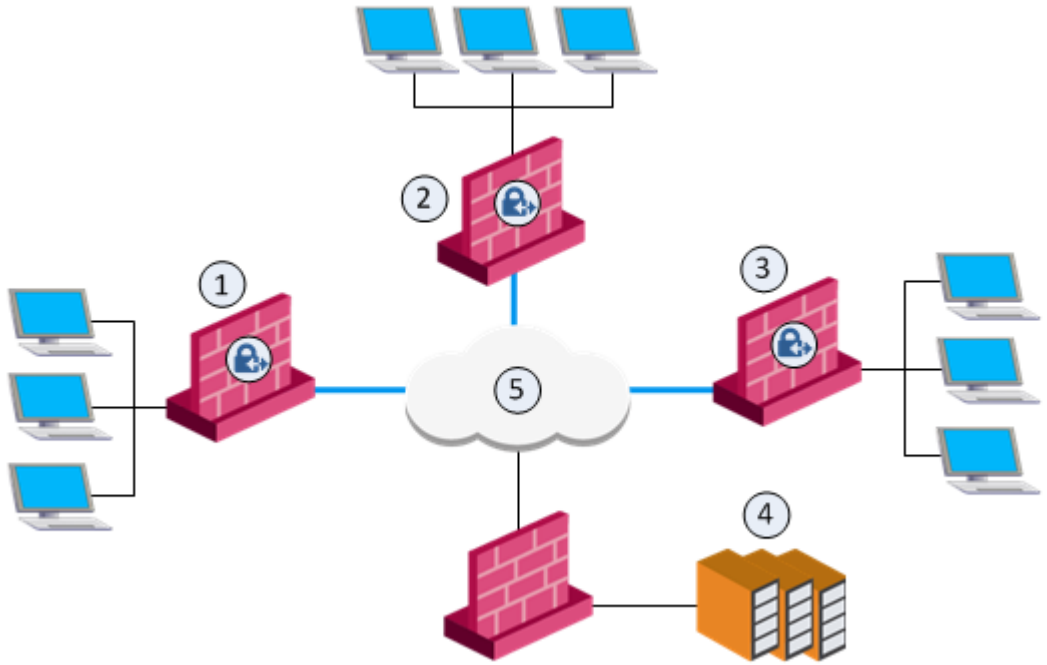
■ 各Security Gatewayが少なくとも1つのルールを実施することを確認します。どのルールも適用されない場合、デフォルトのドロップルールが適用されます。

■ 選択したインストール対象に、ユーザデータベースとオブジェクトデータベースを配布します。

組織内のサイトの種類によって、異なるポリシーパッケージを作成することができます。

例

ある組織に4つの拠点があり、それぞれが独自の要件を備えています。各拠点では、Security GatewayにインストールされているSoftware Bladesのセットが異なっています。



項 目	セキュリティゲート ウェイ	インストールされたSoftware Blade
1	Sales California	ファイアウォール、VPN
2	Sales Alaska	ファイアウォール、VPN、IPS、DLP
3	経 営 陣	ファイアウォール、VPN、QoS、モバイルアクセス
4	サーバファーム	ファイアウォール
5	インターネット	

これらの異なるタイプのサイトを効 率 的に管 理するには、3つの異なるポリシーパッケージを作 成する必 要 があります。各 パッケージには、サイトのSecurity Gatewayにインスト ールされたSoftware Bladeに対 応 するポリシータイプの組 み合 わせが含 まれています。例 :

- アクセスコント ロールポリシータイプを含 むポリシーパッケージ。アクセスコント ロールポリシータイプは、ファイアウォール、NAT、アプリケーションコント ロールとURLフィルタリング、およびコンテンツ認 識 の各 Software Bladesを制 御します。このパッケージは、VPN構 成も決 定します。

  すべてのセキュリティゲート ウェイにアクセスコント ロールポリシーパッケージをインスト ールします。

- 帯 域を管 理するSecurity Gateway上 のQoSブレード のQoSポリシータイプを含 むポリシーパッケージです。

  このポリシーパッケージを*エグゼクティブ管 理*セキュリティゲート ウェイにインスト ールします。

- モバイルアクセスを扱うセキュリティゲート ウェイ用 のデスクトップセキュリティのポリシータイプ を含 むポリシーパッケージです。

  このポリシーパッケージを*エグゼクティブ管 理* セキュリティゲート ウェイにインスト ールします。

新しいポリシーパッケージの作 成

1. メニューから、**Manage policies and layers**を選 択します。

   Manage policies and layersウィンド ウが開きます。

2. **New**をクリックします。

   New Policyウィンド ウが開きます。

3. ポリシーパッケージの名 前を入 力します。

4. **General**ページ > **Policy types**セクションで、これらのポリシータイプを1つ以 上 選 択します:

   - **Access Control & HTTPS Inspection**
   - **Threat Prevention**
   - **QoS**、**Recommended**を選 択 または**Express**
   - **Desktop Security**

   QoS、および**Desktop Security**のポリシータイプを表 示 するには、1台 以 上 のゲート ウェイ でこれらを有 効 にします。

   ゲート ウェイ エディタ >**General Properties** >**Network Security** タブを開きます:

   - Qoの場 合 : **QoS**
   - デスクトップセキュリティの場 合 、**IPSec VPN**を選 択し**Policy Server**

5. **Installation targets**ページで、ポリシーがインスト ールされるゲート ウェイを選 択します。

   - **All gateways**
   - **Specific gateways**- 各 ゲート ウェイの [+] 記 号 をクリックし、リスト から選 択します。

   ポリシーパッケージを正 しくインスト ールし、エラーをなくすために、各 ポリシーパッケージは適 切 なインスト ールターゲット のセット と関 連 付 けられています。

6. クリック**OK**。

7. クリック**Close**。

   新しいポリシーは、**Security Policies**ページに表 示 されます。

既 存 のポリシー パッケージにポリシー タイプを追 加 する

1. メニューから、**Manage policies and layers**を選 択します。

   Manage policies and layersウィンド ウが開きます。

2. ポリシーパッケージを選 択し、**Edit**ボタンをクリックします。
3. **New Policy**パッケージのウィンドウが開きます。
4. **General >Policy types** ページで、追 加するポリシータイプを選 択します:
   - **Access Control & HTTPS Inspection**
   - **Threat Prevention**
   - **QoS**、**Recommended**を選 択または**Express**
   - **Desktop Security**
5. クリック**OK**。

ポリシー・パッケージのインストール

1. グローバルツールバーで、**Install Policy**をクリックします。

   Install Policyウィンドウが開き、インストール先 (Security Gateways) が表 示されます。
2. **Select a policy**メニューから、ポリシーパッケージを選 択します。
3. パッケージで利 用 可 能 な1つまたは複 数 のポリシータイプを選 択します。
4. **Install Mode**を選 択します。
   - **Install on each selected gateway independently**- 各 ターゲット ゲート ウェイに他 のゲート ウェイから独 立してポリシーをインストールし、そのうちの1台 でインストールが 失 敗しても、残りのターゲット ゲート ウェイへのインストールに影 響しないようにしま す。

     注 - **For Gateway clusters install on all the members, if fails do not install at all**を選 択した場 合 、Security Management Serverは、インストールの開 始 前 にす べてのクラスタメンバにポリシーをインストールできることを確 認します。1つのメンバに ポリシーをインストールできない場 合 、すべてのメンバに対してポリシーのインスト ール に失 敗します。
   - **Install on all selected gateways, if it fails do not install on gateways of the same version**- すべてのターゲット ゲート ウェイにポリシーをインストールします。1つの ゲート ウェイでポリシーのインストールに失 敗した場 合 、他 のターゲット ゲート ウェイに はポリシーがインストールされません。
5. クリック**Install**。

ユーザデータベースのインストール

SmartConsoleでユーザ定義に変更を加えると、Security Management Server上のユーザデータベースに保存されます。ユーザの認証方法、暗号化キーもこのデータベースに保存されます。ユーザデータベースには、Security Gatewayの外部で定義されたユーザ(外部User Directoryグループのユーザなど)についての情報は含まれて**いません**が、外部グループそのものについての情報(外部グループがどのAccount Unitで定義されているかなど)は含まれています。外部グループへの変更は、ポリシーがインストールされた後、またはユーザデータベースがSecurity Management Serverからダウンロードされた後に有効になります。

変更した内容に応じて、ポリシーまたはユーザデータベースのどちらをインストールするかを選択する必要があります。

- インストール対象で使用されるポリシーパッケージの追加コンポーネントを変更した場合(新しいセキュリティポリシールールの追加など)、ポリシーをインストールします。
- ユーザ定義または管理者定義の変更のみを行った場合は、ユーザデータベースをインストールします。**Install Database**

ユーザデータベースのインストール先:

- セキュリティゲートウェイ - ポリシーインストール時。
- Management Software Bladeが1つ以上有効になっているCheck Pointホスト - データベースのインストール時。

Security Management Server上のコマンドラインインタフェースから、Security GatewayやLog Serverなどのリモートサーバにユーザデータベースをインストールすることも可能です。

コマンドラインインタフェースからユーザデータベースをインストールするには

Security Management Server上で、エキスパートモードで実行します。

```
fwm dbload <Main IP address of Name of Security Gateway Object>
```

詳細は次を参照: *R82 CLI Reference Guide*- *Security Management Server*コマンドの章 - セクション*fwm* - サブセクション*fwm dbload*。

注 - Management Software Bladeがアクティブでない Check Point ホストには、ユーザデータベースはインストールされません。

アクセスコントロールポリシーのアンインストール

セキュリティゲートウェイのコマンドラインインタフェースを使用して、アクセスコントロールポリシーをアンインストールできます。

アクセスコントロールポリシーをアンインストールするには

1. Security Groupでコマンドラインに接続します。
2. エキスパートモードにログインします。
3. 次を実行します:

```
fw unloadlocal
```

警告

- "`fw unloadlocal`"コマンドは、セキュリティゲートウェイ(クラスタメンバ)上のLinuxカーネルのIP Forwardingを無効にするため、すべてのトラフィックがセキュリティゲートウェイ(クラスタメンバ)を通過しないようにします。
- "`fw unloadlocal`"コマンドは、セキュリティゲートウェイ(クラスタメンバ)からすべてのポリシーを削除します。つまり、セキュリティゲートウェイ(クラスタメンバ)が、フィルタリングや保護を有効にすることなく、すべてのアクティブなインタフェースを宛先とするすべての着信接続を受け入れます。

詳細は次を参照: *R82 CLI Reference Guide*- *セキュリティゲートウェイコマンド*の章 - セクション*fw* - サブセクション*fw unloadlocal*。

その他のセキュリティポリシーのアンインストールについては、関連する管理者ガイドを参照してください。

ルールログの表 示

特 定 のルールによって生 成されたログは、セキュリティポリシーから、またはログとイベント > **Logs** タブから検 索 できます。

ルールで生 成されたログを見 るには(セキュリティポリシーから)

1. SmartConsoleで、**Security Policies**ビューに移 動します。
2. **Access Control Policy**または**Threat Prevention Policy**で、ルールを選 択します。
3. 下 のペインで、これらのタブのいずれかをクリックして表 示します。
   - **Logs**- デフォルトでは、*現在 のルール*のログが表 示されます。**Source**,**Destination**,**Blade**,**Action**,**Service**,**Port**,**Source Port**,**Rule** (**Current rule**がデフォルト) ,**Origin**,**User**, または**Other Fields**でフィルタリング可 能 です。
   - **History**(アクセスコントロールポリシーのみ) - ルールに関 連 するルール操 作 (監 査 ログ) を時 系 列 にリストし、ルールの種 類 と変 更 を行った管 理 者 の情 報 を表 示します。

ルールで生 成されたログを見 るには(ログ検 索)

1. SmartConsoleで、**Security Policies**ビューに移 動します。
2. **Access Control Policy**または**Threat Prevention Policy**で、ルールを選 択します。
3. ルール番 号 を右 クリックし、**Copy Rule UID**を選 択します。
4. Logs & Events >**Logs** タブで、以 下 のいずれかの方 法 でログを検 索します:
   - ルールUIDをクエリ検 索 バーに貼 り付 け、Enterキーを押します。
   - より速く結 果 を得 るには、クエリ検 索 バーでこの構 文 を使 用します。

     ```
     layer_uuid_rule_uuid:*_<UID>
     ```

     例 えば、クエリの検 索 バーにこれを貼 り付 けてEnterキーを押します。

     ```
     layer_uuid_rule_uuid:*_46f0ee3b-026d-45b0-b7f0-5d71f6d8eb10
     ```

ポリシーインストール履歴

ポリシーのインストール履歴の操作方法

インストール履歴では、セキュリティゲートウェイ、ポリシーがインストールされた日時を選択できます。また、以下を実行できます。

- セキュリティゲートウェイにインストールされたリビジョンと、誰がポリシーをインストールしたかを確認する。
- インストールされた変更と、誰が変更したかを確認する。
- 特定のバージョンに戻し、最後の"適切な"ポリシーをインストールする。

ポリシーのインストール履歴を操作するには

1. SmartConsoleで、**Security Policies**にアクセスします。
2. **Access Tools**または**Threat Prevention Tools**から、**Installation History**を選択します。
3. **Gateways**セクションで、セキュリティゲートウェイを選択します。
4. **Policy Installation History**セクションで、インストール日を選択します。
5. 該当するアクションを実行します。
   - **インストールされたリビジョンとその作成者を確認するには**

     View installed changesをクリックします。
   - **インストールされた変更と変更者を確認するには**

     Viewをクリックします。
   - **ポリシーの特定のバージョンに戻すには**

     Install specific versionをクリックします。

同時インストールポリシー

R81から、1人以上の管理者が複数のゲートウェイで同時に*異なる*ポリシーのインストールタスクを実行できるようになりました。以前のバージョンでは、複数のゲートウェイで*同じ*ポリシー インストールタスクを同時に実行することしかできませんでした。

同時インストールポリシーでは、アクセスコントロールとThreat Preventionのポリシーのみがサポートされています。デスクトップやQoSのポリシーには対応していません。

異なるポリシーのインストールタスクを同時に実行できる最大数は5です。5つ以上のポリシーインストールがリクエストされた場合は、最初の5件以降の要求はキューに入れられます。

実行中のタスクとキューに入れられたタスクは、画面左下のRecent Tasksウィンドウに表示されます。

注 - 最初のインストールでは、同じゲートウェイにアクセス制御とThreat Preventionの両方のポリシーを同時にインストールすることはできません。どちらかをインストールしてから、もう一方をインストールする必要があります。

Accelerated Install Policy

R81では、アクセスコントロールポリシーにAccelerated Install Policy機能が導入されました。アクセスコントロールポリシーのインストールを高速化すると、インストール時間が大幅に短縮されます。

ポリシーのインストールは、前回のインストール以降にアクセスコントロールポリシーに対して行われた変更に応じて加速されます。

たとえば、Hostオブジェクトを作成してアクセスコントロールルールに追加すると、ポリシーのインストールが*加速されます*。

アクセラレートインストールポリシーの詳細と、アクセラレートポリシーインストールのトリガとなるイベントの詳細リストについては、sk169096を参照してください。

アクセスコントロールポリシーの作成

このセクションでは、アクセスコントロールポリシーを使用するための手順を説明します。

統合アクセスコントロールポリシーの導入

1つの統一されたアクセスコントロールポリシーを定義します。アクセスコントロールポリシーでは、これらすべてのアクセスコントロール機能を組み合わせた、シンプルできめ細かいルールベースを作成することができます。

- ファイアウォール - 内部ネットワークへのアクセスおよび内部ネットワークからのアクセスを制御します。
- アプリケーションとURLフィルタリング - アプリケーションとサイトをブロックします。
- コンテンツアウェアネス - ユーザがアップロードまたはダウンロードできるデータタイプを制限することができます。
- IPsec VPNとモバイルアクセス - Site-to-Site VPNとRemote Access VPNで安全な通信を設定します。
- アイデンティアウェアネス - ユーザ、コンピュータ、ネットワークを識別します。

ルールベースを個別に管理する必要はありません。たとえば、次のような直感的なルールを定義できます: 指定されたネットワークのユーザには、指定されたアプリケーションの使用を許可するが、指定されたサイズを超えるファイルのダウンロードは禁止する。次のオブジェクトはすべて1つのルールで使用することができます。

- セキュリティゾーン
- サービス
- アプリケーションとURL
- データタイプ
- アクセスロール

次の機能に関する情報は、1つのログとして収集されます。

- ネットワーク
- プロトコル
- アプリケーション
- ユーザ
- アクセスしたリソース
- データタイプ

アクセスコントロールルールベースのカラム

これらは、アクセスコントロールポリシーのルールカラムです。デフォルトでは、すべてが表示されるわけではありません。表示されないカラムを選択するには、ルールベースのヘッダを右クリックして選択します。

カラム	説明
No	ルールベースレイヤのルール番号。
Hits	接続がルールにマッチした回数。 参照: *ルールベースのヒットカウントの分析 (400ページ)*。
Name	システム管理者がこのルールに付ける名前。
Source Destination	次を定義するネットワークオブジェクト: ■ トラフィックが始まる場所 ■ トラフィックの宛先 参照: *送信元と送信先のカラム (328ページ)*。
VPN	ルールが適用されるVPNコミュニティ。 参照: *VPNカラム (328ページ)*。
Services & Applications	サービス、アプリケーション、カテゴリ、サイト。 アプリケーション& URLフィルタリングが有効でない場合は、サービスのみが表示されます。 参照: *サービス& アプリケーションカラム (330ページ)*。
Content	保護するデータアセット(クレジットカード番号や医療記録など)。 データの方向は、Download Traffic(組織内)、Upload Traffic(組織外)、Any Directionのいずれかに設定できます。 参照: *コンテンツカラム (334ページ)*。
Action	トラフィックがルールに一致したときに実行されるアクション。オプション: Accept、Drop、Ask、Inform(UserCheckメッセージ)、Inline Layer、Reject。 参照: *アクション (335ページ)*。
Track	トラフィックがルールに一致したときに行われるアクションを追跡し、ログに記録します。 参照: *追跡カラム (337ページ)*。
Install On	ポリシーのルールを取得するネットワークオブジェクト。 参照: *アクセスコントロールポリシーのインストール (395ページ)*。

カラム	説明
Time	このルールが適用される期間。
Comment	ルールを要約するオプションのフィールド。

送信元と送信先のカラム

アクセスコントロールポリシールールベースの送信元カラムと宛先カラムには、あらゆるタイプのグループを含む**ネットワーク**オブジェクトを追加できます。

ここでは、設定可能なネットワークオブジェクトを紹介します。

- ネットワーク(*ネットワーク (284ページ)*と*ネットワークグループ (285ページ)*)
- ホスト
- ゾーン(*セキュリティゾーン (304ページ)*)
- ダイナミックオブジェクト (*ダイナミックオブジェクト (301ページ)*)
- ドメインオブジェクト*ドメイン (294ページ)*)
- アクセスロール
- 更新可能オブジェクト (*更新可能なオブジェクト (295ページ)*)

ネットワークオブジェクトについての詳細

アクセスコントロールポリシーの**Source**と**Destination**カラムにネットワークオブジェクトを追加できます。参照: *オブジェクトの管理 (279ページ)*。

VPNカラム

サイト間VPN、リモートアクセスVPN、モバイルアクセスポータルおよびクライアントに対するルールを設定できます。

VPNコミュニティのルールを作成するには、このカラムにSite-to-Site CommunityまたはRemote Access VPN Communityオブジェクトを追加するか、**Any**を選択してすべてのVPNコミュニティにルールを適用させます。

セキュリティゲートウェイでMobile Accessを有効にすると、セキュリティゲートウェイは自動的に**RemoteAccess** VPNコミュニティに追加されます。ルールの**VPN**カラムにそのコミュニティを含めるか、**Any**を使用して、ルールをモバイルアクセスセキュリティゲートウェイに適用させることができます。セキュリティゲートウェイがVPNコミュニティから削除された場合、**VPN**カラムに**Any**を含める必要があります。

IPsec VPN

IPsec VPNソリューションは、セキュリティゲートウェイが他のセキュリティゲートウェイやクライアントとの間でトラフィックを暗号化および復号できるようにします。SmartConsoleを使用して、セキュリティゲートウェイとリモートデバイス間のVPN接続を簡単に設定できます。

サイト間コミュニティでは、VPNネットワークにスター型トポロジとメッシュ型トポロジを設定し、サードパーティゲートウェイを含めることができます。

VPNトンネルでは次を確実に行います。

- 認証 - 標準的な認証方法を使用
- プライバシー - VPNデータはすべて暗号化
- 整合性 - 業界標準の整合性保証方式を採用

IKEとIPsec

Check PointのVPNソリューションは、安全なVPNプロトコルを使用して暗号化キーを管理し、暗号化されたパケットを送信します。IKE (Internet Key Exchange) は、VPNトンネルを作成するために使用される標準的な鍵管理プロトコルです。IPsecは、プライベートネットワークやパブリックネットワーク上で認証・暗号化された安全なIP通信をサポートするプロトコルです。

ネットワークへのモバイル・アクセス

Check Pointのモバイルアクセスを使用することで、リモートユーザがインターネットを利用して簡単かつ安全に社内ネットワークに接続できます。リモートユーザは、Mobile Access Security Gatewayに対して標準的なHTTPSリクエストを開始し、1つまたは複数の安全な認証方式で認証を行います。

モバイルアクセスポータルは、モバイルワーカーやリモートワーカーがインターネット経由で重要なリソースに簡単かつ安全に接続することを可能にします。Check Pointのモバイルアプリは、管理されていないスマートフォンやタブレットから企業のリソースへの安全な暗号化通信を可能にします。アクセスには、社内アプリ、メール、カレンダー、連絡先などがあります。

モバイルアクセスアプリケーションへのアクセスをルールベースに含めるには、**Services & Applications**カラムに**Mobile Application**を含めます。

指定したリモートアクセスクライアントを介してリソースにアクセスできるようにするには、クライアント用のアクセスロールを作成し、ルールの**Source**カラムに含めます。

VPNの詳細について

サイト間VPNとリモートアクセスVPNの詳細については、次のガイドを参照してください。

- *R82 Site to Site VPN Administration Guide*
- *R82 Remote Access VPN Administration Guide*
- *R82 Mobile Access Administration Guide*

サービス& アプリケーションカラム

アクセスコントロールルールベースのServices & Applicationsカラムで、ルールに含まれるアプリケーション、サイト、およびサービスを定義します。ルールには、1つまたは複数の以下を含めることができます。

- サービス
- アプリケーション
- モバイルアクセスのアプリケーション
- Webサイト
- インターネットトラフィックのデフォルトのカテゴリ
- Check Pointのアプリケーションデータベースには含まれない、ユーザが作成したカスタムグループ/カスタムカテゴリ。

サービスマッチング

セキュリティゲートウェイは、*IPプロトコル*、TCPおよびUDP*ポート番号*、*プロトコルシグネチャ*に従ってサービスを識別(マッチング)します。

セキュリティゲートウェイがプロトコルシグネチャでサービスを照合できるようにするには、セキュリティゲートウェイと順序レイヤーでApplication & URL Filteringを有効にする必要があります(参照)。*アクセスコントロール機能の有効化 (363ページ)*)。

TCPおよびUDPサービスを*ソースポート*でマッチングするように設定できます。

アプリケーションマッチング

ポリシーでアプリケーションが*許可*されている場合、ルールはアプリケーションのRecommended サービスにのみマッチします。このデフォルト設定は、すべてのサービスでアプリケーションを許可するよりも安全です。たとえば、Facebookを許可するルールは、アプリケーションコントロールWeb Browsing Services:`http`、`https`、`HTTP_proxy`、`HTTPS_proxy`上でのみ許可します。

ポリシーで*ブロックされている*アプリケーションは、すべてのサービスでブロックされます。そのため、すべてのポートでブロックされます。

アプリケーションのデフォルトのマッチング設定は変更できます。

許可されたアプリケーションのマッチング設定

ルールがポリシーで*許可*されているアプリケーションまたはカテゴリとどのように一致するかを設定できます。アプリケーションにマッチするルールは、次のいずれかの方法で設定できます。

- 任意のサービス
- 特定のサービス

そのためには、アプリケーションまたはカテゴリのMatch Settingsを変更します。アプリケーションまたはカテゴリは、ポリシーで使用されているすべての場所で変更されます。

許可されたアプリケーションまたはカテゴリのサービスを変更するには

1. Services & Applicationsカラムにアプリケーションまたはカテゴリがあるルールで、アプリケーションまたはカテゴリをダブルクリックします。
2. Match Settingsを選択します。
3. オプションを選択します。
   - デフォルトは、Recommendedサービスです。Webサービスのデフォルトは、アプリケーションコントロールWeb Browsing Services 。
   - アプリケーションとすべてのサービスを一致させるには、Anyをクリックします。
   - 指定したサービスでアプリケーションを一致させるには、Customizeをクリックし、サービスを追加または削除します。
   - アプリケーションをすべてのサービスと一致させ、特定のサービスを除外するには、Customizeをクリックし、除外するサービスを追加して、Negateを選択します。
4. クリックOK。

ブロックされたアプリケーションのマッチング設定

デフォルトでは、ポリシーでアプリケーションが*ブロックされる*と、すべてのサービスでブロックされます。そのため、すべてのポートでブロックされます。

ブロックされたアプリケーションのマッチングを推奨サービス上で行うように設定できます。Webアプリケーションの場合、推奨サービスは*アプリケーションコントロールのWebブラウジングサービス*です。

アプリケーションのマッチ設定がCustomizeに設定されている場合、ブロックされたアプリケーションはカスタマイズされたサービスサービスでマッチングされます。*すべてのポートでマッチするわけではありません。*

ブロックされたアプリケーションのマッチングを設定するには

1. SmartConsoleで次にアクセスします: Manage & Settings > Blades > Application & URL Filtering > Advanced Settings > Application Port Match
2. Match application on 'Any' port when used in 'Block' ruleを設定します:
   - 選択済み - これがデフォルトです。ルールベースでアプリケーションが*ブロックされている*場合、アプリケーションは*任意*のポートにマッチします。

- 選択されていない - アプリケーションがルールベースで*ブロックされ*ている場合、アプリケーションは、アプリケーションのアプリケーションオブジェクトで設定されているサービスに一致します。ただし、一部のアプリケーションはAny(任意)でマッチングされます。標準的なサービスセットに制限されないアプリケーション(Skypeなど)がこれに当たります。

ブロックルールのアプリケーションマッチングのサマリ

アプリケーション - マッチング設定	チェックボックス: ブロックルールで使用する場合、「任意の」ポートのWebアプリケーションに一致させます。	ブロックされたアプリケーションはサービスで一致
推奨サービス(デフォルト)	選択(デフォルト)	Any
推奨サービス(デフォルト)	未選択	推奨サービス
カスタマイズ	*関連なし*	カスタマイズ
Any	*関連なし*	Any

ルールにサービス、アプリケーション、サイトを追加する

ルールにサービス、アプリケーション、サイトを追加できます。

注:アプリケーションまたはカテゴリによるルールは、セキュリティゲートウェイからの接続またはセキュリティゲートウェイへの接続には適用されません。

サービス、アプリケーション、またはサイトをルールに追加するには

1. SmartConsoleのセキュリティポリシービューで、**Access Control**Policyに移動します。
2. アプリケーションをルールに追加するには、**Applications and URL Filtering**が有効なレイヤを選択します。
3. ルールの**Services & Applications**セルを右クリックし、**Add New Items**を選択します。
4. サービス、サイト、アプリケーション、カテゴリを検索します。
5. 追加する対象の横にある**+**をクリックします。

カスタムアプリケーション、カテゴリ、グループの作成

Check Pointのアプリケーションデータベースには含まれないカスタムアプリケーション、カテゴリ、またはグループを作成できます。

アプリケーションやサイトを新規に作成するには

1. SmartConsoleのセキュリティポリシービューで、**Access Control**Policyに移動します。
2. **Applications and URL Filtering**が有効になっているレイヤーを選択します。
3. ルールの**Services & Applications**セルを右クリックし、**Add New Items**を選択します。

   アプリケーションビューアのウィンドウが開きます。
4. **New** >**Custom Applications/Site** >**Application/Site**をクリックします。
5. オブジェクトの名前を入力します。
6. 1つまたは複数のURLを入力します。

   URLに正規表現を使用した場合は、**URLs are defined as Regular Expressions**をクリックします。

   注 - アプリケーションまたはサイトのURLが正規表現で定義されている場合、正しい構文を使用する必要があります。sk165094を参照してください。
7. クリック**OK**。

カスタムカテゴリを作成するには

1. SmartConsoleのセキュリティポリシービューで、**Access Control**Policyに移動します。
2. **Applications and URL Filtering**が有効になっているレイヤーを選択します。
3. ルールの**Services & Applications**セルを右クリックし、**Add New Items**を選択します。

   アプリケーションビューアのウィンドウが開きます。
4. **New** > **Custom Applications/Site** > **User Category**をクリックします。
5. オブジェクトの名前を入力します。
6. オブジェクトの説明を入力します。
7. クリック**OK**。

R77.30以下のセキュリティゲートウェイにおけるサービスとアプリケーション、およびアップグレード後について

Security Gateway R77.30以下の場合：

- セキュリティゲートウェイは、TCPおよびUDPサービスを*ポート*番号でマッチングします。Security Gatewayはプロトコル署名でサービスを照合できません。
- Security Gatewayは、アプリケーションの署名によってアプリケーションを照合します。

Security Management ServerをR80以降に、Security GatewayをR80.10以降にバージョンアップすると、この動作が変更されます。

- アプリケーション＆ URLフィルタリングルールベースで定義されたアプリケーションは、推奨ポートで許可されます。

コンテンツカラム

アクセスコントロールポリシーのルールの「コンテンツ」カラムにデータタイプを追加できます。

「コンテンツ」カラムを使用するには、セキュリティゲートウェイの一般プロパティページで、**Content Awareness**を有効にし、レイヤー上で使用する必要があります。

データタイプはデータの分類です。ファイアウォールは、データタイプに従って着信トラフィックと発信トラフィックを分類し、それに応じてポリシーを適用します。

ポリシーのデータの方向は、**Download Traffic**(組織内)、**Upload Traffic** (組織外)、または**Any Direction**に設定できます。

データタイプには2種類あります: *コンテンツタイプ*(ファイルの内容を分析して分類) と*ファイルタイプ* (ファイルIDを分析して分類) です。

コンテンツタイプの例 :

- PCI - クレジットカード番号
- HIPAA - 医療記録番号 - MRN
- 国際銀行口座番号 - IBAN
- ソースコード - JAVA
- 米国の社会保障番号 - SSAによる
- 給与調査用語

ファイルタイプの例 :

- ビューアファイル - PDF
- 実行ファイル
- データベースファイル
- ドキュメントファイル
- プレゼンテーションファイル
- 表計算ファイル

注

- Content Awareness Software Bladeは、すべてのポートで HTTP、HTTPS、SMTP、FTP プロトコルをサポートしています。アクセスコントロール統一ルールベースと完全に統合されています。
- Content Awareness Software Bladeは、バイナリ証明書*.cerファイルを「証明書と秘密鍵」のデータタイプにマッチさせません。
- コンテンツアウェアネスとDLP(Data Loss Prevention) は、どちらもデータタイプを使用します。しかし、両者には異なる特徴や機能があります。それぞれ独立して動作し、セキュリティゲートウェイで別々に実施されます。
- インラインレイヤの親ルールのコンテンツカラムに**Archive File** 、サブルールのコンテンツカラムに別の値 (例: Presentation File)がある場合、マッチしたアーカイブに別の値 (この例ではプレゼンテーションファイル)が含まれていると、そのルールはマッチしません。両方のコンテンツタイプに通常のルールを使用します。
- ルールのコンテンツカラムに、**Compound Data Type Group**または**Traditional Data Type Group**と、**Archive File**データタイプおよび別のデータタイプ (例:**PCI - Credit Card Numbers**) が含まれる場合、クレジットカードを含むファイルを含むアーカイブファイルがアップロードまたはダウンロードされると、そのルールは一致しません。
- コンテンツカラムに**Archive File**を持つルールがマッチし、ルールベースの下位ルールがアーカイブファイルに含まれるデータタイプを持つ場合、ルールベースの下位ルールもマッチします。

制限:

- Content Awarenessは、日本語、韓国語、ギリシャ語、アラビア語を含む、テキストファイル用の60以上の文字セット(charset) をサポートしています。検査されたトラフィックにサポートされている文字セットが含まれていない場合、Content AwarenessはデコードにUTF-8を使用します。サポートされている文字セットのリストと、デフォルトの文字セットを変更する方法については、sk116155を参照してください。
- Content Awarenessは、ファイル名に基づくデータタイプをサポートしています。ファイル名がURLまたはcontent-dispositionヘッダの一部でない特定のHTTPトラフィックでは、ファイル名が正しくない可能性があります。

データタイプの詳細については、SmartConsoleでデータタイプのオブジェクトを開き、**?**ボタン (または**F1**キー) を押してヘルプを確認します。

DLPの詳細: *R82 Data Loss Prevention Administration Guide*。

アクション

アクション	意味
Accept	トラフィックを許可
Drop	トラフィックを破棄します。セキュリティゲートウェイは接続の発信側に応答を送信せず、接続は最終的にタイムアウトを起こします。このアクションにUserCheckオブジェクトが定義されていない場合、ページは表示されません。

アクション	意味
Ask	ユーザに質問し、確認用のチェックボックス、または理由ボックスを追加します。UserCheckオブジェクトを使用します。
Inform	アプリケーションやコンテンツにアクセスしようとするユーザに対して、メッセージを送信します。UserCheckオブジェクトを使用します。
これらのアクションを確認するには、右クリックして**More**を選択：	
Reject	トラフィックを拒否します。セキュリティゲートウェイは接続元に対してRSTパケットを送信し、接続を終了します。
UserCheck Frequency	アクションが「Ask」、「Inform」、「Block」のとき、ユーザが設定したメッセージを見る頻度を設定します。
Confirm UserCheck	UserCheckメッセージのトリガとなるアクションを選択します。 ■ **Per rule**- UserCheckメッセージは、トラフィックがルールに一致した場合に一度だけ表示されます。 ■ **Per category**- UserCheckメッセージは、ルールの各マッチングカテゴリに表示されます。 ■ **Per application/Site**- UserCheckメッセージは、ルール内の一致するアプリケーション/サイトごとに表示されます。 ■ **Per Data type**- UserCheckメッセージは、一致するデータタイプごとに表示されます。
Limit	ルールに許可される帯域幅を制限します。 **Limit**オブジェクトを追加して、アップロードとダウンロードの最大スループットを設定します。 **重要：** ポリシーのインストール後、これらのシナリオのいずれかでアクション"**Limit**"を持つアクセスコントロールルールに一致する接続に帯域幅の制限が適用されません。 ■ セキュリティオブジェクトで'**Keep all connections**'オプションが選択されています。 ■ このルールで使用されるサービスオブジェクトでは、'**Keep connections open after the policy has been installed**'オプションが選択されています。
Enable Identity Captive Portal	HTTPトラフィックを認証(Captive)ポータルにリダイレクトします。ユーザが認証された後、このソースからの新しい接続は、認証を必要とせずに検査されます。 **重要** - **Source**および**Destination**パラメータを**Any**と定義してトラフィックをドロップするルールは、Captive Portalへのトラフィックとそこからのトラフィックもドロップします。

追跡カラム

Trackingのオプションには次のようなものが含まれます。

- None- ログを生成しない。
- Log- これはデフォルトのTrackオプション。セキュリティゲートウェイが接続をマッチングするために使用したすべての情報が表示されます。
- Accounting- これを選択すると、10分間隔でログが更新され、接続中にどれだけのデータが経過したかが表示されます: アップロードバイト、ダウンロードバイト、ブラウズ時間。

追跡(トラッキング)の詳細について

トラッキングオプションの詳細: *R82 Logging and Monitoring Administration Guide*。

アクセスコントロールポリシーのルールマッチング

セキュリティゲートウェイは、接続に適用するルールを決定します。これをコネクションのマッチングと呼びます。セキュリティゲートウェイでの接続のマッチング方法を理解することで、次のようなことに役立ちます。

- ルールベースからより良いパフォーマンスを実現する。
- 接続が一致したことを示すログを理解する。

ルールマッチングの例

以下のルールベース例では、セキュリティゲートウェイがどのように接続をマッチングさせるかを示しています。

これらのルールベースは、意図的にアクセスコントロールルールのベストプラクティスに従っていないことに注意してください (*アクセスコントロールルールのベストプラクティス (370ページ)*)。これは、ルールマッチングの説明をわかりやすくするためです。

ルールベースマッチング - 例1

このルールベースの場合：

いいえ	発信元	宛先	サービス & アプリケーション	内容	アクション
1	InternalZone	インターネット	ftp-pasv	実行ファイルのダウンロード	ドロップ
2	Any	Any	Any	実行ファイル	承認
3	Any	Any	ギャンブル(カテゴリ)	Any	ドロップ
4	Any	Any	Any	Any	承認

FTP接続時のマッチング手順：

接続の一部	セキュリティゲートウェイのアクション	検査結果
SYN	ルールベースを実行：マッチする最初のルールを探す： ■ ルール1 - 一致。	最後のマッチ(ルール1でドロップ) 。 ログに表示。 セキュリティゲートウェイは、他のルールのインスペクションエンジンをオンにしません。

ルールベースマッチング - 例2

このルールベースの場合:

No.	発信元	宛先	サービス & アプリケーション	内容	アクション
1	InternalZone	インターネット	Any	実行ファイルのダウンロード	ドロップ
2	Any	Any	ギャンブル(カテゴリ)	Any	ドロップ
3	Any	Any	ftp	Any	ドロップ
4	Any	Any	Any	Any	承認

ファイル共有Webサイトを閲覧する際のマッチング方法です。上から下へ列を進みます。各列を左から右へ進みます。

接続の一部	セキュリティゲートウェイのアクション	検査結果
SYN	ルールベースを実行。 マッチする最初のルールを探す: ■ ルール1 - 一致の可能性。 ■ ルール2 - 一致の可能性。 ■ ルール3 - 一致なし。 ■ ルール4 - 一致。	一致の可能性(接続の検査を続行) 。
HTTP ヘッダ	セキュリティゲートウェイは、インスペクションエンジンをオンにして、接続中のデータを検査します。 この例では、次をオンにします。 ■ URLフィルタリングエンジン - ギャンブルサイトかどうか。 ■ コンテンツアウェアネスエンジン - 実行可能ファイルかどうか。	アプリケーション: ファイル共有 (カテゴリ)。 内容: 不明。

接続の一部	セキュリティゲートウェイのアクション	検査結果
	ルールベースのマッチングを最適化する。 マッチする最初のルールを探す: ■ ルール1 - 一致の可能性。 ■ ルール2 - 一致なし。 ■ ルール3 - 一致なし。 ■ ルール4 - 一致。	一致の可能性(接続の検査を続行)。
HTTP本文	ファイルを調べる。	データPDFファイル
	ルールベースのマッチングを最適化する。 マッチする最初のルールを探す: ■ ルール1 - 一致なし。 ■ ルール2 - 一致なし。 ■ ルール3 - 一致なし。 ■ ルール4 - 一致。	最終マッチ(ルール4で許可)。 ログに表示。

ルールベースマッチング - 例3

このルールベースの場合:

No.	発信元	宛先	サービス アプリケーション	内容	アクション
1	InternalZone	インターネット	Any	実行ファイルのダウンロード	ドロップ
2	Any	Any	ギャンブル(カテゴリ)	Any	ドロップ
3	Any	Any	Any	Any	承認

企業Webサイトから実行ファイルをダウンロードする際のマッチング手順です。上から下へ列を進みます。各列を左から右へ進みます。

接続の一部	セキュリティゲートウェイのアクション	検査結果
SYN	ルールベースを実行。 マッチする最初のルールを探す: ■ ルール1 - 一致の可能性。 ■ ルール2 - 一致の可能性。 ■ ルール3 - 一致。	一致の可能性(接続の検査を続行)。
HTTPヘッダ	セキュリティゲートウェイは、インスペクションエンジンをオンにして、接続中のコンテンツを検査します。 この例では、次をオンにします。 ■ URLフィルタリングエンジン - ギャンブルサイトかどうか。 ■ コンテンツアウェアネスエンジン - 実行可能ファイルかどうか。	アプリケーション:ビジネス(カテゴリ)。 内容:不明。
	ルールベースのマッチングを最適化する。 マッチする最初のルールを探す: ■ ルール1 - 一致の可能性。 ■ ルール2 - 一致なし。 ■ ルール3 - 一致。	一致の可能性(接続の検査を続行)。
HTTP本文	ファイルを調べる。	内容:実行ファイル。
	ルールベースのマッチングを最適化する。 マッチする最初のルールを探す: ■ ルール1 - 一致。 ■ ルール2 - 一致なし。 ■ ルール3 - 一致。	最後のマッチ(ルール1でドロップ)。 ログに表示。

マッチングの例では:

- セキュリティゲートウェイではルールベースが複数回実行されることがあります。実行のたびに、セキュリティゲートウェイはマッチングを最適化し、接続に適用される最初のルールを見つけます。
- ルールにアプリケーション、サイト、またはプロトコル署名(**Application and Services**カラム)、データタイプ(**Content**カラム)を持つサービスが含まれている場合、セキュリティゲートウェイは:

- 1つまたは複数のインスペクションエンジンをオンにします。
- 接続の本体を検査するまで、最終的なマッチング判定を延期します。

■ セキュリティゲートウェイは、接続に適用されます(マッチする) 最初のルールを検索します。セキュリティゲートウェイが一致するルールを特定するために必要なすべての情報を持っていない場合、トラフィックの検査を続行します。

基本的なアクセスコントロールポリシーの作成

セキュリティゲートウェイは、アクセスコントロールルールベースを構成する一連のルールを使用して、コンピュータ、クライアント、サーバ、およびアプリケーションへのアクセスを制御します。安全なアクセスコントロールと最適化されたネットワークパフォーマンスを実現するルールベースを構成する必要があります。

強力なアクセスコントロールルールベースで、以下を実現します。

- 許可された接続のみをアクセス許可し、ネットワークの脆弱性を防止する。
- 許可されたユーザに適切な社内リソースへのアクセスを与える。
- 接続を効率的に検査する。

基本ルール

ベストプラクティス - これらは、すべてのルールベースに対して推奨される基本的なアクセスコントロールルールです。

- セキュリティゲートウェイへの直接アクセスを防止する**ステルスルール**
- ポリシー内の以前のルールでマッチしないすべてのトラフィックをドロップする**クリーンアップルール**

使用例 - 基本的なアクセスコントロール

このユースケースは、単純なアクセスコントロール セキュリティポリシーのルールベースを示しています。(**Hits**, **VPN**, **Content**のカラムは非表示)。

いいえ	名前	発信元	宛先	サービス&アプリケーション	アクション	追跡	インストール先
1	セキュリティゲートウェイへの管理者アクセス	Admins (アクセスロール)	セキュリティゲートウェイのグループ	Any	承認	ログ記録	ポリシーの対象
2	ステルス	Any	セキュリティゲートウェイのグループ	Any	ドロップ	アラート	ポリシーの対象
3	クリティカルサブネット	内部	ファイナンス HR 研究開発	Any	承認	ログ記録	CorpGW

いいえ	名前	発信元	宛先	サービス&アプリケーション	アクション	追跡	インストール先
4	テクニカルサポート	テックサポート	リモート1-web	HTTP	承認	アラート	リモート1GW
5	DNSサーバ	Any	DNS	ドメインUDP	承認	なし	ポリシーの対象
6	メールサーバ、Webサーバ	Any	DMZ	HTTP HTTPS SMTP	承認	ログ記録	ポリシーの対象
7	SMTP	メール	内部ではないネットグループ	SMTP	承認	ログ記録	ポリシーの対象
8	DMZとインターネット	IntGroup	Any	Any	承認	ログ記録	ポリシーの対象
9	クリーンアップルール	Any	Any	Any	ドロップ	ログ記録	ポリシーの対象

ルールについての説明：

ルール	説明
1	**Admin Access to Gateways**- SmartConsoleの管理者は、セキュリティゲートウェイへの接続が許可されます。
2	**Stealth**- SmartConsole管理者からセキュリティゲートウェイのいずれかに接続されていない内部トラフィックはすべてドロップされます。接続がステルスルールに一致すると、SmartView Monitorに警告ウィンドウが表示されます。
3	**Critical subnet**- 内部ネットワークから指定されたリソースへのトラフィックが記録されます。このルールでは、3つのサブネットをクリティカルリソースと定義しています(財務、人事、研究開発)。
4	**Tech support**- テクニカルサポートサーバから、リモートワンセキュリティゲートウェイの背後にあるリモートワンWebサーバへのアクセスを許可します。HTTPトラフィックのみ許可されます。パケットがTech supportルールに一致した場合、アラートアクションが実行されます。
5	**DNS server**- 外部DNSサーバへのUDPトラフィックを許可します。このトラフィックはログに記録されません。

ルール	説明
6	**Mail and Web servers**- DMZにあるメールサーバとWebサーバへの受信トラフィックを許可します。HTTP、HTTPS、SMTPのトラフィックが許可されます。
7	**SMTP**- メールサーバへの送信SMTP接続を許可します。危険なメールサーバの侵入を防ぐため、内部ネットワークへのSMTP接続は許可しません。
8	**DMZ and Internet**- 内部ネットワークからDMZおよびインターネットへのトラフィックを許可します。
9	**Cleanup rule**- 先のルールのいずれかにマッチしないすべてのトラフィックをドロップします。

使用例 - 各部門のインラインレイヤー

この使用例では、各部門のサブポリシーを持つ基本的なアクセスコントロールポリシーを示しています。各部門のルールは、インラインレイヤーになっています。インラインレイヤーは、ルールベースの他の部分から独立しています。異なるレイヤーの所有権を異なる管理者に委任することができます。

いいえ	名前	発信元	宛先	サービス&アプリケーション	内容	アクション	追跡
1	クリティカルサブネット	内部	ファイナンス HR	Any	Any	承認	ログ記録
2	SMTP	メール	内部ネットワークではない(グループ)	smtp	Any	承認	ログ記録
3	研究開発部門	研究開発のロール	Any	Any	Any	テックサポートレイヤー	N/A
3.1	研究開発サーバ	Any	R&Dサーバ(グループ) QAネットワーク	Any	Any	承認	ログ記録

いいえ	名前	発信元	宛先	サービス&アプリケーション	内容	アクション	追跡
3.2	研究開発ソース管理	InternalZone	ソースコントロールサーバ(グループ)	ssh http https	Any	承認	ログ記録
---	---	---	---	---	---	---	---
3.X	クリーンアップルール	Any	Any	Any	Any	ドロップ	ログ記録
4	QA部門	QAネットワーク	Any	Any	Any	QAレイヤー	N/A
4.1	研究開発サーバへのアクセスを許可する	Any	R&Dサーバ(グループ)	Web サービス	Any	承認	ログ記録
---	---	---	---	---	---	---	---
4.Y	クリーンアップルール	Any	Any	Any	Any	ドロップ	ログ記録
5	すべてのユーザの従業員ポータルアクセスを許可	Any	従業員ポータル	Web サービス	Any	承認	なし
---	---	---	---	---	---	---	---
9	クリーンアップルール	Any	Any	Any	Any	ドロップ	ログ記録

ルールについての説明 :

ルール	説明
1 2	組織全体の一般ルール

ルール	説明
3 3.1 3.2 --- 3.X	研究開発部門のインラインレイヤー。 ルール3は、インラインレイヤーの親ルールです。**Action**は、インラインレイヤーの名前です。 **パケットが親ルール3にマッチしない場合：** マッチングはインラインレイヤーの外側にある次のルール(ルール4) に続きます。 **パケットが親ルール3にマッチした場合：** マッチングは3.1まで続き、インラインレイヤー内の最初のルールになります。パケットがこのルールにマッチした場合、そのパケットに対してルールアクションが実行されます。 パケットがルール3.1にマッチしない場合、インラインレイヤー内の次のルールであるルール3.2に進みます。一致しない場合、インラインレイヤーの残りのルールに進みます。---は、1つ以上のルールを意味します。 パケットはインラインレイヤーの内部でのみマッチングされます。インラインレイヤーには暗黙のクリーンアップルールがあるため、インラインレイヤーから離れることはありません。 ルール4、5、およびOrdered Layerの他のルールではマッチングされません。 ルール3.Xは、**cleanup rule**です。インラインレイヤーの先のルールのいずれかにマッチしないトラフィックをすべてドロップします。これはデフォルトの明示的ルールです。ルールは変更または削除することができます。 **ベストプラクティス** - インラインレイヤーと順序レイヤーの最後に、明示的なクリーンアップルールを設定します。
4 4.1 --- 4.Y	QA部門の、もう1つのインラインレイヤー。
5	より一般的な組織全体のルール。
--	1つまたは複数のルール。
9	**Cleanup rule**- Ordered Layerの先のルールのどれかにマッチしないトラフィックをすべてドロップします。これはデフォルトの明示的ルールです。ルールは変更または削除することができます。 **ベストプラクティス** - インラインレイヤーと順序レイヤーの最後に、明示的なクリーンアップルールを設定します。

セルのデフォルト値

R81.10以降:

- 新規ルールのSource,Destination、Services & Applicationsカラムのデフォルト値は"None"です。

  R81以前のバージョンでは、新規ルールのこれらのカラムのデフォルト値は"Any"です。

- セルから最後のオブジェクトを削除した後のセルのデフォルト値は"None"です。

  「最後のオブジェクト」とは、他のオブジェクトがすべて削除された後、セル内の最後のオブジェクトとして残ったオブジェクトです。

  R81以前のバージョンでは、セルから最後に削除されたオブジェクトのデフォルト値は"Any"です。

To configure the default values for the Source, Destination, and Services & Applications columns:

1. Manage & Settingsビュー > **Policy Settings** > **Rule Base Cell Settings**
2. **Security Access Defaults**で、ソース、宛先、サービス& アプリケーションのカラムの値を選択

セルから最後のオブジェクトを削除した後に、ソース、宛先、サービス& アプリケーションのカラムの値を構成するには:

1. Manage & Settingsビュー >**Policy Settings** > **Rule Base Cell Settings**
2. **After removing the last object in a cell**セクションで、以下のいずれかを選択します。
   - **Add 'None' to the cell**- セルから最後のオブジェクトを削除すると、セルの値は"None"になります。
   - **Add the object according to the Rule Base cell default**- セル内の最後のオブジェクトを削除すると、セルの値は**Security Access Defaults**セクションで設定した値になります。

注 - セルを右クリックすると、"Any"と"None"が切り替わります。

値 "None"を持つルールの実行

バージョンR80.10～R81のSecurity Gatewayでは、1つ以上のセルに値「**None**」を含むルールがインストールされません。

ルールが"None"のときに表示するメッセージを設定するには

管理と設定 >**Policy Settings** > ルールベース**Cell Settings** > に移動**'None' object behavior**

R81以前のManagement Serverからのアップグレード

R81以前のバージョンからのアップグレード時

- **Source**、**Destination**、**Services & Applications**カラムのデフォルト値は、"**Any**"のままです。
- セル内の最後のオブジェクトが削除された後のデフォルト値は"**None**"になります。

アプリケーションコントロールとURLフィルタリングのルールの作成

SmartConsoleのAccess Controlビューのアクセスコントロールポリシーで、アプリケーションコントロールとURLフィルタリングのポリシーを作成し、管理します。アプリケーションコントロールとURLフィルタリングのルールは、どのユーザが組織内から特定のアプリケーションやサイトを利用できるか、またどのようなアプリケーションやサイトの利用がログに記録されるかを定義します。

どのアプリケーションやカテゴリが高リスクであるかを知るには、Security PoliciesビューのAccess Tools部分にあるApplication Wikiに目を通してください。ポリシーに盛り込むべきアプリケーションやカテゴリのアイデアを探します。

アクセスコントロールポリシーとトラフィックの概要を見るには、Access Control >Logs & Events > New TabのViewsビューを参照してください。

ベストプラクティスアプリケーションコントロールとURLフィルタリングを同じルールで使用しないでください。ルールが正しく一致しなくなる場合があります。アプリケーションコントロールとURLフィルタリングは別々のルールで使用します。これにより、カテゴリが特定されると同時に、URLフィルタリングルールが使用されるようになります。詳細は、sk174045を参照してください。

セキュリティゲートウェイ/クラスタメンバがインターネットに直接接続されていない場合、管理サーバをプロキシサーバとして使用し、アプリケーションコントロールパッケージとURLフィルタリングパッケージを更新します。

この機能はデフォルトで有効になっています。

- この機能を無効にするには、セキュリティゲートウェイ/各クラスタメンバのエキスパートモードで実行します。

  ```
  cpprod_util FwSetParam CP_BLADE_UPDATE_PROXY_MGMT_DISABLE 1
  ```

- この機能を再度有効にするには、セキュリティゲートウェイ/各クラスタメンバのエキスパートモードで実行します:

  ```
  cpprod_util FwSetParam CP_BLADE_UPDATE_PROXY_MGMT_DISABLE 0
  ```

アプリケーションのモニタリング

シナリオ: 組織内のすべてのFacebookトラフィックをモニタしたい。どうすればよいですか?

すべてのFacebookアプリケーションのトラフィックを監視するには

1. SmartConsoleのセキュリティポリシービューで、Access ControlPolicyに移動します。
2. Applications and URL Filteringが有効になっているレイヤーを選択します。

3. **Add rule**ツールバーボタンのいずれかをクリックすると、ルールベース内で選択した位置にルールが追加されます。最初にマッチしたルールが適用されます。
4. 次のコンポーネントを含むルールを作成します。
   - **Name**- **Monitor Facebook**といった名前をルールに付けます。
   - **Source**- 組織からのすべてのトラフィックに適用されるよう、**Any**として保持します。
   - **Destination**- インターネットまたはDMZに向かうすべてのトラフィックに適用されるよう、**Internet**としておきます。
   - **Services & Applications**- プラス記号をクリックしてアプリケーションビューアを開きます。ルールに**Facebook**のアプリケーションを追加します。
     a. 検索フィールドに「face」と入力していきます。利用可能なリストに**Facebook**アプリケーションが表示されます。
     b. 各項目をクリックすると、説明ペインに詳細が表示されます。
     c. ルールに追加する項目を選択します。

     注- アプリケーションは、デフォルトで**推奨**サービスにマッチングされます。これを変更することができます (*許可されたアプリケーションのマッチング設定 (330ページ)*)。各サービスは特定のポートで実行されます。推奨する**Web Browsing Services**は、`http`、`https`、`HTTP_proxy`、`HTTPS_proxy`です。
   - **Action**- 選択 : **Accept**
   - **Track**- 選択 : **Log**
   - **Install On**- すべてのセキュリティゲートウェイを**Policy Targets** 、または特定のセキュリティゲートウェイを選択してルールをインストールします。

このルールは、すべてのFacebookトラフィックを許可し、ログ記録します。ログは**Logs & Events**ビューの**Logs**タブで見ることができます。組織内のFacebookの利用状況を監視するには、**Access Control**ビュー(SmartEvent Serverが必要) を確認します。

アプリケーションのブロックとユーザへの通知

シナリオ: 組織内でポルノサイトをブロックし、違反についてユーザに伝えたい。どうすればよいですか?

アプリケーションまたはアプリケーションのカテゴリをブロックし、ポリシー違反についてユーザに伝えるには

1. SmartConsoleのセキュリティポリシービューで、**Access Control**Policyに移動します。
2. **Applications and URL Filtering**が有効になっているレイヤーを選択します。
3. 次のコンポーネントを含むルールを作成します。

- **Services & Applications**- **Pornography**カテゴリを選択します。
- **Action**- **Drop**、UserCheck**Blocked Message - Access Control**

  メッセージは、ユーザの行為が会社のポリシーに反していることを知らせるとともに、Webサイトが誤ったカテゴリに含まれている場合に報告するためのリンクを含めることができます。
- **Track**-**Log**

  注 - このルールベース例には、ここに関連するカラムのみが含まれています。

名前	発信元	宛先	サービス&アプリケーション	アクション	追跡	インストール先
ポルノをブロック	Any	インターネット	ポルノ(カテゴリ)	ドロップ ブロック・メッセージ	ログ記録	ポリシーの対象

このルールは、ポルノサイトへのトラフィックをブロックし、それらのサイトへのアクセス試行をログに記録します。ルールに違反したユーザには、会社のセキュリティポリシーに基づきアプリケーションがブロックされたことを知らせるUserCheckメッセージが表示されます。メッセージには、Webサイトが不正なカテゴリに含まれている場合に報告するためのリンクを含めることができます。

重要 - **Source**および**Destination**パラメータが**Any**として定義されているトラフィックをブロックするルールは、Captive Portalへのトラフィックおよび Captive Portalからのトラフィックもブロックします。

アプリケーショントラフィックの制限

シナリオ: 業務に支障をきたさないよう、従業員のストリーミングメディアへのアクセスを制限したい。

アプリケーションやカテゴリをブロックしたくない場合、従業員のアクセス制限を設定するさまざまな方法があります。

- ルールに**Limit**オブジェクトを追加して、ルールに許可される帯域幅を制限します。
- ルールに1つまたは複数の**Time**オブジェクトを追加して、指定した時間帯のみアクティブにすることができます。

例として、次のようなルールがあります。

- ピーク時以外の営業時間内に限り、ストリーミングメディアへのアクセスを許可する。
- 社内のストリーミングメディアのアップロードスループットを1Gbpsに制限する。

時間と帯域幅の制限付きでストリーミングメディアを許可するルールを作成するには

1. SmartConsoleのセキュリティポリシービューで、**Access Control**Policyに移動します。
2. **Applications and URL Filtering**が有効になっているレイヤーを選択します。
3. **Add Rule**ツールバーボタンのいずれかをクリックすると、ルールベース内で選択した位置にルールが追加されます。
4. 次のコンポーネントを含むルールを作成します。
   - **Services & Applications**- **Media Streams**カテゴリ

     注 - アプリケーションは**推奨**サービス上でマッチングされ、各サービスは特定のポートで実行されます。例えば、デフォルトのアプリケーションコントロール**Web browsing Services**:`http`、`https`、`HTTP_proxy`、`HTTPS_proxy`、`quic`。変更するには: *サービス & アプリケーションカラム (330ページ)*。
   - **Action**- **More**をクリックし、**Action**:*Accept*、**Limit**オブジェクトを選択します。
   - **Time**- ルールが有効な時間または期間を指定する**Time**オブジェクトを追加します。

     注 - **Time**カラムは、デフォルトではルールベーステーブルに表示されません。これを見るには、テーブルのヘッダを右クリックし、**Time**を選択します。

名前	発信元	宛先	サービスとアプリケーション	アクション	追跡	インストール先	時間
ストリーミングメディアの制限	Any	インターネット	メディアストリーム(カテゴリ)	承認 Upload_1Gbps	ログ記録	すべて	営業時間外

重要:

- ClusterXL負荷分散モードでは、指定された帯域幅の上限は、クラスタの状態に関係なく、構成されたすべてのクラスタメンバ間で分割されます。たとえば、最大制限要件が30 Gbpsで、クラスタメンバが3人いる場合、ルールのLimitオブジェクトを30 Gbps / 3 = 10 Gbpsに設定する必要があります。
- Scalable Platform Security Groupでは、状態に関係なく、指定された帯域幅制限がすべてのセキュリティグループメンバ間で分割されます。例えば、最大制限要件が30 Gbpsで、セキュリティグループメンバが3人いる場合、ルールのLimitオブジェクトを30 Gbps / 3 = 10 Gbpsに設定する必要があります。

ルールにおけるアイデンティティ認識機能の使用

シナリオ: 指定したユーザグループにはリモートアクセスアプリケーションを許可し、その他のユーザには同じアプリケーションをブロックしたい。他のリモートアクセスアプリケーションもブロックしたい。どうすればよいですか?

セキュリティゲートウェイで Identity Awareness を有効にすると、アプリケーションコントロールと併用して、*アクセスロール*に適用するルールを作成できます。アクセスロールオブジェクトを使用して、ユーザ、マシン、ネットワークロケーションを1つのオブジェクトとして定義します。

この例では

- 組織内のすべての識別されたユーザを表すアクセスロール**Identified_Users**はすでに作成されています。セキュリティゲートウェイ上で識別されたユーザのみにアプリケーションへのアクセスを許可するために使用できます。
- すべてのユーザに対して Radminリモートアクセスツールへのアクセスを許可したい。
- 組織内のすべてのユーザに対して、他のすべてのリモートアクセスツールをブロックしたい。また、リモート接続やリモートコントロールを確立できる他のアプリケーションもブロックしたい。

これらを実現するには、2つの新しいルールをルールベースに追加します。

1. ルールを作成し、次のコンポーネントを含めます。
   - **Source- Identified_Users**アクセスロール
   - **Destination-Internet**
   - **Services & Applications - Radmin**
   - **Action-Accept**
2. 下に別のルールを作成し、次のコンポーネントを含めます。
   - **Source-Any**
   - **Destination-Internet**

- **Services & Applications**- カテゴリ: **Remote Administration**
- **Action**-**Block**

名前	発信元	宛先	サービス&アプリケーション	アクション	追跡	インストール先
識別されたユーザにRadminを許可	Identified_Users	インターネット	Radmin	許可	ログ記録	すべて
他のリモート管理者をブロック	Any	インターネット	リモート管理	ブロック	ログ記録	すべて

これらのルールに関する注意事項:

- Radminを許可するルールは他のリモート管理ツールをブロックするルールよりも上位にあるため、最初にマッチングされます。
- 最初のルールのソースは**Identified_Users**のアクセスロールです。テクニカルサポート部門を表すアクセスロールを使用する場合、テクニカルサポート部門のユーザのみがRadminを使用することが許可されます。
- アプリケーションは**推奨**サービスに基づいてマッチングされ、各サービスは特定ポートで実行されます。例: デフォルトのアプリケーションコントロール **Web browsing services**: `http`、`https`、`HTTP_proxy`、`HTTPS_proxy`、`quic`。これを変更するには、「アプリケーションとカテゴリのサービスの変更」を参照してください。

アクセスロールとアイデンティティアウェアネスについては、以下を参照してください。*R82 Identity Awareness Administration Guide*。

サイトのブロック

シナリオ: 責任問題を引き起こす可能性のあるカテゴリに関連するサイトをブロックしたい。これらのカテゴリのほとんどはアプリケーションデータベースに存在するが、カスタム定義されたサイトも含みたい。どうすればよいですか?

*カスタムグループ*を作成し、該当するすべてのカテゴリとサイトをそのグループに追加することでこれを行うことができます。セキュリティゲートウェイで Identity Awareness を有効にすると、URL フィルタリングと一緒に使用して、*アクセスロール*に適用するルールを作成できます。アクセスロールオブジェクトを使用して、ユーザ、マシン、ネットワークロケーションを1つのオブジェクトとして定義します。

この例では

- 以下が既に作成されています。
  - 組織内のすべての識別されたユーザ(*Identified_Users*) を表すアクセスロール。
  - *FreeMovies*というサイトのカスタムアプリケーション。
- 組織内のすべての人に責任問題を引き起こす可能性のあるサイトをブロックしたい。

- アプリケーションデータベースカテゴリと、以前に定義した*FreeMovies*というカスタムサイトを含むカスタムグループを作成します。

カスタムグループを作成するには

1. オブジェクトエクスプローラで、**New > More > Custom Application/Site > Application/Site Group**をクリックします。
2. グループに名前をつけます。例 : *Liability_Sites*
3. **+**をクリックして、グループメンバを追加します。
   - カスタムアプリケーション*FreeMovies*を検索し、追加します。
   - **Categories**を選択し、ブロック対象を追加します(例 : *Anonymizer*、*Critical Risk*、*Gambling*) 。
   - クリック**Close**
4. クリック**OK**。

これで、アクセスコントロールルールベースで*Liability_Sites*グループを使用できるようになります。

ルールベースに、以下のようなルールを追加します。

SmartConsoleのセキュリティポリシービューで、**Access Control**Policyに移動します。

- **Source- Identified_Users**アクセスロール
- **Destination-Internet**
- **Services & Applications-** *Liability_Sites*
- **Action-Drop**

  注 - アプリケーションは、**推奨される**サービスにマッチします。各サービスは、デフォルトのApplication Control**Web Browsing Services**:`http,https,HTTP_proxy,HTTPS_proxy` のように、特定のポートで実行されます。これを変更するには、「アプリケーションとカテゴリのサービスの変更」を参照してください。

名前	発信元	宛先	サービス&アプリケーション	アクション	追跡
法的責任の発生する可能性のあるサイトをブロック	Identified_Users	インターネット	Liability_Sites	ドロップ	ログ記録

URLカテゴリのブロック

シナリオ: ポルノサイトをブロックしたい。どうすればよいですか?

そのためには、ポルノを含むすべてのサイトを*ポルノ カテゴリ*でブロックするルールを作成します。セキュリティゲートウェイで Identity Awareness を有効にすると、URL フィルタリングと一緒に使用して、*アクセスロール*に適用するルールを作成できます。アクセスロールオブジェクトを使用して、ユーザ、マシン、ネットワークロケーションを1つのオブジェクトとして定義します。

この例では

- 組織内のすべての識別されたユーザを表すアクセスロール(*Identified_Users*) を作成済みです。
- ポルノ関連のサイトをブロックしたい。

手順 : *アプリケーションのブロックとユーザへの通知 (351ページ)*。

オーダーレイヤーとインラインレイヤー

ポリシーとは、セキュリティゲートウェイが送受信トラフィックに適用するルールのセットです。アクセスコントロールと脅威対策には、それぞれ異なるポリシーがあります。

アクセスコントロールルールは、Ordered LayersとInline Layersを使用して、より管理しやすいルールのサブセットに整理することができます。

オーダレイヤーとインラインレイヤーの必要性

オーダーレイヤーとインラインレイヤーにより、サイバーセキュリティの管理を効率的に行うことができます。以下を実行できます。

- ルールベースを簡素化したり、特定の目的のためにその一部を整理します。
- フラットなルールベースではなく、インラインレイヤーを用いて、ポリシーを階層的に整理します。

  インラインレイヤーはルールベースの残りの部分から独立した*サブポリシー*です。
- Ordered Layersを複数のポリシーパッケージで再利用し、Inline Layersを複数のレイヤーで再利用します。
- 異なるレイヤーの所有権を異なる管理者に与えることで、ポリシーの管理を簡素化することができます。
- レイヤーのルール数を減らすことで、パフォーマンスを向上させます。

インラインレイヤーにおけるルール実行の順序

オーダレイヤーはインラインレイヤーを含むことができます。

インラインレイヤーの例 :

No.	発信元	宛先	VPN	サービス	アクション
1					
2	Lab_network	Any	Any	Any	Lab_rules
2.1	Any	Any	Any	https http	許可
2.2	Any	Any	Any	Any	ドロップ
3					

インラインレイヤーは、親ルール(例ではルール2) とサブルール(ルール2.1、2.2) を持っています。親ルールのアクションは、インラインレイヤーの名前です。

パケットがインラインレイヤーの親ルールにマッチしない場合、オーダレイヤの次のルール(ルール3)にマッチングが行われます。

パケットがインラインレイヤーの親ルール(ルール2)に一致すると、セキュリティゲートウェイはサブルールと照合します。

- パケットがインラインレイヤのサブルール(ルール2.1)にマッチした場合、それ以上のルールマッチは行われません。
- 順序付きレイヤーの上位ルールのいずれもパケットとマッチしない場合、明示的な**クリーンアップルール**が適用されます(ルール2.2)。このルールがない場合、**暗黙のクリーンアップルール**が適用されます(*ルールベースにおけるルールの種類 (364ページ)*)。それ以上のルールマッチングは行われません。

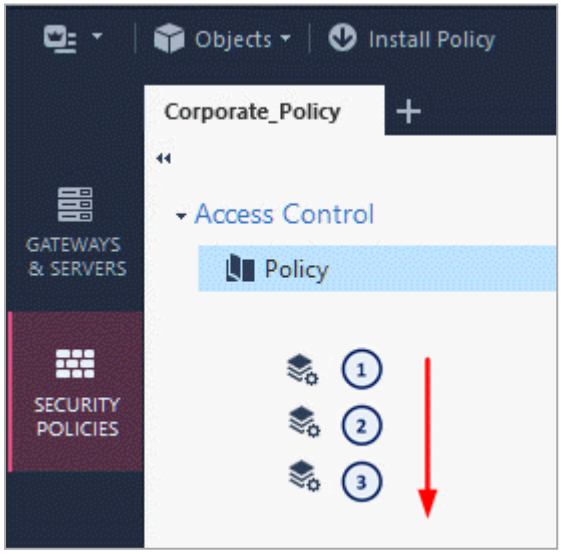
重要:

- 各 Inline Layer の最後には必ず明示的な**クリーンアップルール**を追加し、その**Action**が**Implicit Cleanup Rule**の**Action** と同じであることを確認します。
- Security Gateway R80.10以前では、2番目のレイヤーはアプリケーションコントロールポリシーのように動作します。

Ordered Layersにおけるルール実行の順序

セキュリティゲートウェイにパケットが到着すると、セキュリティゲートウェイはそのパケットを上から順番に最初のOrdered Layerのルールと照合し、パケットにマッチした最初のルールを適用します。

一致するルールの**Action**が**Drop**の場合、セキュリティゲートウェイはポリシールールベースのそれ以降のルールとのマッチングを停止し、パケットをドロップします。**Action**が**Accept**の場合、セキュリティゲートウェイは次のOrdered Layerのルールをチェックし続けます。



項目	説明
1	Ordered Layer 1

項目	説明
2	Ordered Layer 2
3	Ordered Layer 3

Ordered Layerのどのルールもパケットにマッチしない場合、明示的な**Default Cleanup Rule**が適用されます。このルールがない場合、**暗黙のクリーンアップルール**が適用されます(*ルールベースにおけるルールの種類 (364ページ)*)。

すべてのOrdered Layerは、個別の暗黙のクリーンアップルールを持ちます。*Accept*または*Drop*を**Layer settings**で設定できます(*暗黙のクリーンアップルールの設定 (366ページ)*)。

重要 - 各Ordered Layerの最後には必ず明示的な**Cleanupルール**を追加し、その**Action**が**Action**(**Implicit Cleanupルール**) と同じであることを確認してください。

インラインレイヤーの作成

インラインレイヤーは、ルールベースの他の部分とは独立した*サブポリシー*です。

インラインレイヤー作成のワークフローは、以下の通りです。

1. インラインレイヤーの*親ルール*を作成します。インラインレイヤーのすべてのルールに共通するプロパティを1つ以上持つルールを作成します。例えば、同じソースやサービス、またはユーザのグループを持つルール。
2. インラインレイヤーの*サブルール*を作成します。これらは、セキュリティゲートウェイが親ルールへの接続にマッチした場合の処理をより詳細に定義するルールです。例えば、各サブルールは、特定のホスト、ユーザ、サービス、データタイプに適用することができます。

インラインレイヤーを作成するには

1. Ordered Layerにルールを追加します。これは*親ルール*です。
2. **Source**、**Destination**、**VPN**、**Services & Applications**の各セルで、インラインレイヤーのマッチング条件を定義します。
3. ルールの**Action**セルをクリックします。標準的なアクションを選択する代わりに、**Inline Layer** >**New Layer** を選択します。
4. **Layer Editor**ウィンドウが開きます。
5. インラインレイヤーのプロパティを設定します。

a. インラインレイヤーのルールのために、これらのBladesを1つ以上有効にします。

- Firewall
- Application & URL Filtering
- Content Awareness
- Mobile Access

b. **オプション**: 可能であれば、他のポリシーパッケージとレイヤーを共有するのがベストプラクティスです。これを有効にするには、**Multiple policies can use this layer** を選択します。

c. **Advanced**をクリックします。

d. **Implicit Cleanup Rule** を*Drop*または*Accept*に設定します。*ルールベースにおけるルールの種類 (364ページ)*)。

e. クリック**OK**。

インラインレイヤーの名前は、ルールの**Action**セルに表示されます。

6. インラインレイヤーの親ルールの下に、*サブルール*を追加します。
7. インラインレイヤーの最後のルールとして、明示的なクリーンアップルールがあることを確認します (*ルールベースにおけるルールの種類 (364ページ)*)。

注 - リモートアクセスVPNコミュニティオブジェクトは、アクションが "Inline Layer "の場合、Inline Layerの親ルールではサポートされません。
この問題を解決するにはリモートアクセスVPNコミュニティオブジェクトの代わりに、親ルールで「*Any」を使用します。インラインレイヤーのルールで、リモートアクセスVPNコミュニティオブジェクトを使用することができます。

Ordered Layerの作成

オーダーレイヤーを作成するには

1. SmartConsole で、**Menu** >**Manage Policies and Layers** をクリックします。
2. 左側のペインで**Layers**をクリックします。

   レイヤーのリストが表示されます。**Show only shared Layers**を選択できます。
3. 上部にあるツールバーの**New**アイコンをクリックします。
4. **Layer Editor**ウィンドウで設定を行います。
5. **オプション**: 可能であれば、他のポリシーパッケージとレイヤーを共有するのがベストプラクティスです。これを有効にするには、**Multiple policies can use this layer**を選択します。
6. クリック**OK**。
7. クリック**Close**。

8. SmartConsoleセッションを公開する。

   このOrdered Layerはまだポリシーパッケージに割り当てられていません。

アクセスコントロールポリシーにオーダレイヤーを追加するには

1. SmartConsoleで、**Security Policies**をクリックします。
2. アクセスコントロールポリシーセクションのレイヤーを右クリックし、**Edit Policy**を選択します。

   Policyウィンドウが開きます。
3. **Access Control**セクションで、プラス記号をクリックします。

   追加可能なレイヤーのリストが表示されます。これらは、**Multiple policies can use this layer**が有効になっているレイヤーです。
4. レイヤーを選択します。
5. クリック**OK**。
6. SmartConsoleセッションを公開する。

セキュリティゲートウェイR77.30以下：URLフィルタリングとアプリケーションコントロールのレイヤーを作成する場合

1. SmartConsoleで、**Security Policies**をクリックします。
2. **Access Control Policy**セクションのレイヤーを右クリックし、**Edit Policy**を選択します。

   Policyウィンドウが開きます。
3. **Access Control**セクションで、プラス記号をクリックします。
4. **New Layer**をクリックします。

   Layer Editorウィンドウが開き、**General**ビューが表示されます。
5. レイヤーのアプリケーションとURLフィルタリングを有効にします。
   a. レイヤーの名前を入力します。

      Applicationという名前を推奨します。
   b. **Blades**セクションで、「アプリケーション＆ URLフィルタリング」を選択します。
   c. クリック**OK**、**Layer Editor**ウィンドウが閉じます。
   d. クリック**OK**、**Policy**ウィンドウが閉じます。
6. SmartConsoleセッションを公開する。

アクセスコントロール機能の有効化

アクセスコントロールポリシーを作成する前に、ポリシーで使用するアクセスコントロール機能を有効にする必要があります。

以下の機能を有効にします。

- ポリシーをインストールするセキュリティゲートウェイ。
- ポリシーのOrdered LayersとInline Layers。次を有効にすることができます:
  - **Firewall**。これには、VPN (*VPNカラム (328ページ)*)。
  - **Application & URL Filtering**参照 *サービス & アプリケーションカラム (330ページ)*)。
  - **Content Awareness**参照 *コンテンツカラム (334ページ)*)。
  - **Mobile Access**参照 *ネットワークへのモバイル・アクセス (489ページ)*)。

セキュリティゲートウェイでアクセスコントロール機能を有効にする

1. SmartConsoleの左側のナビゲーションパネルから、**Gateways & Servers**をクリックし、セキュリティゲートウェイオブジェクトをダブルクリックします。

   セキュリティゲートウェイの**General Properties**ウィンドウが開きます。
2. ナビゲーションツリーで**General Properties**をクリックします。
3. **Network Security**タブで、アクセスコントロール機能を1つ以上選択します。
   - **IPsec VPN**
   - **Mobile Access**
   - **Application Control**
   - **URL Filtering**
   - **Content Awareness**
   - **Identity Awareness**
4. クリック**OK**。

レイヤーでアクセスコントロール機能を有効にする

Ordered Layerでアクセスコントロール機能を有効にするには

1. SmartConsoleで、**Security Policies**をクリックします。
2. **Access Control**で、**Policy**を右クリックし、**Edit Policy**を選択します。
3. レイヤーのオプション をクリックします。

4. **Edit Layer**をクリックします。

   Layer Editorウィンドウが開き、**General**ビューが表示されます。

5. Ordered Layerで使用する**Blades**を有効にします。

   - **Firewall**。
   - **Application & URL Filtering**
   - **Content Awareness**
   - **Mobile Access**

6. クリック**OK**。

インラインレイヤーでアクセスコントロール機能を有効にするには

1. SmartConsoleで、**Security Policies**をクリックします。
2. Ordered Layerを選択します。
3. インラインレイヤーの親ルールで、**Action** カラムを右クリックし、**Inline Layer** >**Edit Layer** を選択します。
4. インラインレイヤーで使用する**Blades**を有効にします。

   - **Firewall**
   - **Application & URL Filtering**
   - **Content Awareness**
   - **Mobile Access**

   注 - Ordered Layerで有効になっていないBladeは有効にしないでください。

5. クリック**OK**。

ルールベースにおけるルールの種類

ルールベースには、**明示的**、**暗示的**、**暗黙的**の3種類のルールが存在します。

明示的なルール

管理者が明示的に設定するルールで、指定された条件に基づいてトラフィックを許可またはブロックするもの。

重要 -デフォルトのクリーンアップルールは、すべての新しいレイヤーにデフォルトで追加される明示的なルールです。デフォルトのクリーンアップルールは、変更または削除することができます。各レイヤーの最後のルールとして、明示的なクリーンアップルールを設定することをお勧めします。

暗黙のルール

Global properties設定の一部として利用可能で、編集することができないデフォルトのルールです。暗黙のルールの選択とルールベースでの位置の設定のみ可能です。

- **First**- ルールベース内の他のすべてのルール(明示的/暗示的) の前に、最初に適用されます。
- **Last**- ルールベース内の他のすべてのルール(明示的/暗示的) の後に、最後に適用されます。**Implicit Cleanup Rule**
- **Before Last**- ルールベース内の最後の明示的ルールの前に適用されます

暗黙のルールは、セキュリティゲートウェイが利用するさまざまなサービスの接続を許可するために設定されます。例えば、**Accept Control Connections** のルールは、次のサービスを制御するパケットを許可します。

- セキュリティゲートウェイへのセキュリティポリシーのインストール
- セキュリティゲートウェイからSecurity Management Serverへのログの送信
- RADIUSやTACACS認証サーバなど、サードパーティのアプリケーションサーバへの接続

暗黙のクリーンアップルール

レイヤーのデフォルトの「キャッチオール」ルールは、レイヤー内のどの明示的または暗示的ルールにも一致しないトラフィックを処理します。これは、レイヤーを作成する際に自動的に作成されます。

暗黙のクリーンアップルールは、ルールベースに表示されません。

Security Gateways R80.10以降では、暗黙のクリーンアップルールのデフォルトのアクションは**Drop**です。これは、ほとんどのポリシーがAllow Listルール(Acceptアクション) を持っているからです。レイヤーにブラックリストルール(ドロップアクション) がある場合、レイヤーエディタで暗黙のクリーンアップルールのアクションを「**Accept**(許可) 」に変更することができます。

Security Gateway R77.30以前では、暗黙のルールの動作はOrdered Layerに依存します。

- **ドロップ** - **Network**レイヤー用
- **Accept** - **Applications and URL Filtering**が有効になっているレイヤーの場合。

注 - デフォルト値を変更した場合、Security Gateway R77.30以下ではポリシーのインストールに失敗します。

セキュリティゲートウェイがルールを適用する順序

1. **最初の暗黙のルール** - このルールの前に明示的なルールは置けません。
2. **明示的ルール** - これは管理者が作成するルール。
3. **Before Last Implied Rules** - 最後の明示的ルールの前に適用されます。

4. **最後の明示的ルール** - 最後の明示的ルールとして、**クリーンアップルール**を使用することをお勧めします。

   注 - **クリーンアップルール**を最後の明示的ルールとして使用する場合、**最後の暗黙的ルール**と**暗黙的なクリーンアップルール**は実行されません。

5. **最後の暗黙のルール** - このルールは他のすべての明示的および暗黙のルールの後に適用されますが、暗黙のクリーンアップルールが一番最後に適用されることを忘れないでください。

6. **暗黙のクリーンアップルール** - レイヤーのルールがどれも一致しない場合に適用されるデフォルトのルール。

暗黙のルールの設定

一部の暗黙ルールは、デフォルトで有効になっています。必要に応じて、デフォルトの設定を変更できます。

暗黙ルールを設定するには

1. SmartConsoleで、Access Control Policyを選択します。
2. ポリシーの上にあるツールバーから、**Actions** >**Implied Rules** を選択します。

   Implied Policyウィンドウが開きます。
3. 左側のペインで**Configuration**をクリックします。
4. ルールを選択すると有効になり、ルールをクリアすると無効になります。
5. 有効なルールについては、ルールベース内のルールの位置を選択します: **First**,**Last**, **Before Last** (*ルールベースにおけるルールの種類 (364ページ)*)。
6. クリック**OK**ポリシーをインストールします。

暗黙のルールの表示

SmartConsole の**Security Policies** ビューから**Actions** >**Implied Rules** を選択します。

Implied Policyウィンドウが開きます。

暗黙ルールだけが表示され、明示的なルールは表示されません。

暗黙のクリーンアップルールの設定

暗黙のクリーンアップルールを設定するには

1. SmartConsole で、**Menu** >**Manage Policies and Layers** をクリックします。
2. 左側のペインで**Layers**をクリックします。
3. レイヤーを選択し、**Edit**をクリックします。

Layer Editorが開きます。

4. クリック**Advanced**
5. **Implicit Cleanup Rule**を*Drop*または*Accept*に設定します。
6. クリック**OK**。
7. クリック**Close**。
8. SmartConsoleセッションを公開する。

アクセスコントロールレイヤーの管理者

アクセスコントロールのロール専用の管理者アカウントを作成し、独自のインストール権限とSmartConsoleの読み取り/書き込み権限を持たせることができます。

また、異なるレイヤーの所有権を異なる管理者に委任することも可能です。参照: *アクセスコントロールレイヤーの権限の設定 (120ページ)*。

レイヤーの共有

ポリシーの異なる部分で同じルールを使用したり、複数のポリシーパッケージで同じルールを持つことが必要な場合があります。

何度もルールを作成する必要はありません。Ordered LayerやInline Layerを1度だけ定義し、共有としてマークします。そして、Inline LayerやOrdered Layerを複数のポリシーパッケージで再利用したり、Inline LayerをOrdered Layer内の複数の場所で使用したりすることができます。例えば、企業の管理者が複数の支店間でルールの一部を共有したい場合などに便利です。

- 時間の節約にもつながり、ミスも防ぐことができます。
- 企業の全支店の共有ルールを変更する場合、変更するのは一度だけです。

レイヤーを共有としてマークするには

1. SmartConsoleで、**Menu** > **Manage policies and layers**をクリックします。
2. 左側のペインで**Layers**をクリックします。
3. **Access Control**または**Threat Prevention**でレイヤーを選択します。
4. 右クリックして、**Edit Layer**を選択します。
5. **Layer Editor**ウィンドウで設定を行います。
6. **General**で、**Multiple policies and rules can use this layer**を選択します。
7. クリック**OK**。
8. クリック**Close**。
9. SmartConsoleセッションを公開する。

脅威対策レイヤーを再利用するには

1. SmartConsole で、**Menu** > **Manage policies and layers** > **Policies**に進みます。
2. 必要なポリシーを右クリックして**Edit**をクリックします。ポリシーのプロパティウィンドウが表示されます。
3. Threat Preventionボックスで、**+** 記号をクリックします。
4. このポリシーパッケージに含めたいレイヤーを選択します。
5. クリック**OK**。
6. ポリシーのプロパティウィンドウを閉じます。
7. SmartConsoleで、ポリシーをインストールします。
8. すべてのポリシーパッケージについて、この手順を繰り返します。

インラインレイヤーと順序レイヤーの例については、以下を参照のこと。*統一ルールベースの使用例 (372ページ)*。

ルールベースのセクションによる視覚的分割

多数のルールを持つポリシーをよりよく管理するために、**セクション**を使用してルールベースをより小さな論理的なコンポーネントに分割することができます。この分割はあくまで視覚的なものであり、異なる**セクション**の管理を異なる管理者に委任することはできません。

レイヤルールを.CSVファイルにエクスポートする

レイヤーのルールは.CSVファイルにエクスポートできます。.CSVファイルは、Microsoft Excelなどの表計算アプリケーションで開いて変更することができます。

レイヤールールを.CSVファイルにエクスポートするには

1. SmartConsole で、**Menu** > **Manage Policies and Layers**をクリックします。

   Manage Layersウィンドウが開きます。
2. **Layers**をクリックします。
3. レイヤーを選択し、**Actions** > **Export selected Layer**をクリックします。
4. パスとファイル名を入力します。

ポリシーとレイヤーの管理

Access Control PolicyでOrdered LayersとInline Layersを操作するには、SmartConsoleで**Menu** > **Manage policies and layers**を選択します。

Manage policies and layersウィンドウが表示されます。

ポリシーパッケージのレイヤーとその属性を確認するには

ウィンドウのLayersペインで次が確認できます。

- Name- レイヤー名
- Number of Rules- レイヤーのルール数
- Modifier- 最後にレイヤ構成を変更した管理者。
- Last Modified- レイヤーが変更された日付。
- Show only Shared Layers- 共有レイヤーはMultiple policies and rules can use this Layerオプションが選択されている (*レイヤーの共有 (367ページ)*)。
- Layer Details
  - Used in policies- レイヤーを使用するポリシーパッケージ
  - Mode:
    - Ordered- 順序レイヤー。マルチドメインセキュリティ管理環境では、グローバルルールと、ローカル、ドメインルールのプレースホルダーが含まれます。
    - Inline- インラインレイヤーはサブポリシーとも呼ばれます。
    - Not in use- ポリシーパッケージで使用されないレイヤ。

レイヤーのルールを確認するには

1. レイヤーを選択します。
2. 右クリックして、Open layer in policyを選択します。

アクセスコントロールルールのベストプラクティス

1. 以下のルールがあることを確認します。
   - セキュリティゲートウェイへの直接アクセスを防ぐステルスルール。
   - ポリシーの以前のルールで許可されていないすべてのトラフィックを破棄するクリーンアップルール。
2. レイヤーを使用して、ルールベースのルールの構造と階層を追加します。
3. 送信元と送信先のIPアドレスとポートのみに基づくすべてのルールを、ルールベースの最上部にあるファイアウォール/ネットワーク順のレイヤーに追加します。
4. 安全なトラフィックを明示的に受け入れるファイアウォール / ネットワークルールを作成し、それ以外のすべてをドロップする*明示的なクリーンアップルール*をOrdered Layerの一番下に追加します。
5. ファイアウォール/ネットワーク順序レイヤーの後に、アプリケーションコントロールの順序レイヤーを作成します。不要なトラフィックや安全でないトラフィックを明示的に破棄するルールを追加します。Ordered Layerの下部に明示的なクリーンアップルールを追加し、それ以外をすべて許可します。

   または、アプリケーションコントロールルールをファイアウォール/ネットワークルールの一部としてインラインレイヤーに配置します。インラインレイヤーの親ルールで、ソースと宛先を定義します。
6. 可能な場合は、順序レイヤーとインラインレイヤーを共有します。
7. ファイアウォール/ネットワークルールの順序レイヤーとアプリケーションコントロールの順序レイヤーがある場合 - アプリケーション、データタイプ、モバイルアクセス要素を検査するすべてのルールを、アプリケーションコントロールの順序レイヤー、またはその次の順序レイヤーに追加します。
8. セキュリティゲートウェイがプロキシサーバの背後にある場合を除き、XFFインスペクションをオフにします。詳しくはsk92839を参照してください。
9. 作業中のルールを無効にします。使用する場合は、ルールを有効にします。

   無効なルールは、セキュリティゲートウェイのパフォーマンスに影響しません。

   ルールを無効にするには、ルールの**No.** カラムを右クリックして**Disable**を選択します。

効率的なルールマッチングのベストプラクティス

1. 送信元、送信先、ポートをチェックするルール(ネットワークルール) は、ルールベースの上位に配置します。

   理由 ネットワークルールのマッチングが早くなり、検査エンジンの起動回数が減ります。

2. アプリケーションやコンテンツ(データタイプ) をチェックするルールは、ネットワークルールの下に配置します。
3. Anyカラムおよび**Source**カラムに **"Destination"** があり、アプリケーションまたはデータタイプがあるルールは定義しないでください。

   例えば、これらのルールは**推奨されません**:

発信元	宛先	サービス& アプリケーション	内容
Any	Any	Facebook	
Any	Any		Credit Card numbers

   代わりに、以下の推奨ルールのいずれかを定義してください。

発信元	宛先	サービス& アプリケーション	内容
Any	Internet	Facebook	
Any	オブジェクト (関連サーバを表す)		Credit Card numbers

   2と3の理由 : アプリケーションコントロールとコンテンツアウェアネスルールは、コンテンツ検査を必要とします。

   つまり、次のことが言えます:

   - セキュリティゲートウェイが接続ヘッダと内容を検査するまで接続は許可されます。
   - パフォーマンスに影響を与える可能性があります。

4. データタイプを持つルールの場合 :

   ファイルタイプをチェックするルールは、コンテンツタイプをチェックするルールよりもルールベースの上位に配置します。参照: *コンテンツカラム (334ページ)*。

   理由 : ファイルタイプはコンテンツタイプよりも早く一致します。

5. アプリケーションコントロールとURLフィルタリングを同じルールで使用しないでください。ルールが正しく一致しなくなる場合があります。アプリケーションコントロールとURLフィルタリングは別々のルールで使用します。これにより、カテゴリが特定されると同時に、URLフィルタリングルールが使用されるようになります。詳細は、sk174045を参照してください。

これらのベストプラクティスの例を確認するには次を参照 : *統一ルールベースの使用例 (372ページ)*と*基本的なアクセスコントロールポリシーの作成 (343ページ)*。

統一ルールベースの使用例

ここでは、アクセスコントロールポリシーに定義できるルールの例を示す使用例をいくつか紹介します。

使用例 - アプリケーションコントロールとコンテンツアウェアネス 順序レイヤー

この例では、統一されたアクセスコントロールポリシーの例を示しています。アプリケーションとコンテンツを1つのOrdered Layerで制御します。

No.	名前	発信元	宛先	VPN	サービス&アプリケーション	内容	アクション	追跡
コンプライアンス全般 (1)								
1	ブロックカテゴリ	Any	インターネット	Any	アノニマイザ 深刻なリスク	Any	ドロップ ブロックメッセージ	ログ記録
危険な実行ファイルのブロック (2)								
2	未分類のサイトやリスクの高いサイトからの実行ファイルのダウンロードをブロック	InternalZone	インターネット	Any	未分類 高リスク	トラフィック ダウンロード 実行ファイル	ドロップ	ログ記録
クレジットカード情報 (3-4)								

No.	名前	発信元	宛先	VPN	サービス&アプリケーション	内容	アクション	追跡
3	金融機関によるクレジットカード番号のアップロードを、HTTPS経由でのみ許可	ファイナンス(アクセスロール)	Webサーバ	Any	https	トラフィックのアップロードPCI - クレジットカード番号	承認	ログ記録
4	会社のWebサーバから他のクレジットカードをブロック	Any	Webサーバ	Any	Any	任意の方向PCI - クレジットカード番号	ドロップ	ログ記録
VPNで機密情報を知らせる (5)								
5	VPNサイトからの機密データについてユーザへ通知	Any	Any	RemoteAccess	Any	任意の方向給与調査レポート	通知	ログ記録
クリーンアップ (6)								
6	クリーンアップルール	Any	Any	Any	Any	Any	承認	ログ記録

ルールについての説明：

ルール	説明
1	**一般的なコンプライアンス**セクション - 許容できないWebサイトやアプリケーションへのアクセスをブロックします。
2	**危険な実行ファイルをブロック**するセクション - 危険性の高い実行ファイルのダウンロードをブロックします。
3-4	**クレジットカードデータ**セクション - クレジットカード番号のアップロードをファイナンス部門のみ許可し、HTTPS経由でのみ実行します。それ以外のクレジットカードはブロックします。
5	**VPNセクションで機密データをブロック**するセクション - 組織のVPN経由で接続したリモートユーザには、情報メッセージが表示されます。
6	**クリーンアップ ルール** - 先のルールのいずれかに一致しないすべてのトラフィックを許可します。

使用例 - Webトラフィック用インラインレイヤー

この使用例では、Webトラフィックを制御するアクセスコントロールポリシーの例を示しています。WebサーバのルールはInline Layerにあります。

いいえ	名前	発信元	宛先	サービス&アプリケーション	内容	アクション	追跡
1	本社WEBトラフィック - プロキシ経由	HQ	プロキシ	Webプロキシ	Any	確認 Webアクセスポリシー Access Noti... 1日1回 アプリごと...	ログ記録
2	インターネットへのプロキシを許可	プロキシ	インターネット	ウェブ	Any	承認	なし

いいえ	名前	発信元	宛先	サービス&アプリケーション	内容	アクション	追跡
3	ローカル支社が直接インターネットにアクセスできるようにする	ローカル支社	インターネット	ウェブ	Any	確認 Webアクセスポリシー Access Noti... 1日1回 アプリごと...	ログ 記録
4	Webサーバ	InternalZone	Webサーバ	ウェブ	Any	Webサーバの保護	N/A
4.1	未承認ブラウザの閲覧をブロック	Any	Any	ネゲート Google Chrome Internet Explorer 11 Firefox Safari	Any	ドロップ	ログ 記録
4.2	クレジットカードのアップロードをHTTPSでのみ行うことをユーザに通知	Any	Any	https	トラフィックのアップロード PCI - クレジットカード番号	通知 Access Noti... 1日1回 アプリごと...	ログ 記録
4.3	クレジットカードのブロック	Any	Any	Any	任意の方向 PCI - クレジットカード番号	ドロップ ブロックメッセージ	ログ 記録

いいえ	名前	発信元	宛先	サービス&アプリケーション	内容	アクション	追跡
4.4	機密コンテンツのダウンロードをブロック	Any	Any	Any	トラフィックのダウンロード HIPAA - 医療記録のヘッダ	ドロップ	ログ記録
4.5	クリーンアップルール	Any	Any	Any	Any	承認	なし
5	PayPalにクレジットカードを送信する際にユーザに確認	InternalZone	インターネット	PayPal	任意の方向 PCI - クレジットカード番号	確認 企業ポリシー Access Noti... 1日1回 アプリごと...	ログ記録
6	クリーンアップルール	Any	Any	Any	Any	ドロップ	ログ記録

ルールについての説明：

ルール	説明
4	インラインレイヤーの親ルールです。**Action**は、インラインレイヤーの名前です。パケットが親ルールにマッチした場合、インラインレイヤのルール4.1にマッチングが続きます。パケットが親ルールにマッチしない場合、ルール5でマッチングが続きます。
4.1 -4.4	パケットがルール4.1にマッチした場合、そのパケットに対してルールアクションが行われ、それ以降のルールマッチは行われません。ルール4.1でパケットがマッチしない場合、ルール4.2へ進みます。インラインレイヤの残りのルールも同じロジックです。
4.5	もし順序レイヤーのどの上位ルールもパケットにマッチしない場合、明示的な*クリーンアップルール*が適用されます。*クリーンアップルール*は、デフォルトの明示的ルールです。ルールは変更または削除することができます。各インラインレイヤーと順序レイヤーの最後のルールとして、明示的なクリーンアップルールを設定することをお勧めします。

使用例 - コンテンツアウェアネス順序レイヤー

この例では、組織からのデータのアップロードとダウンロードを制御するポリシーを示しています。

ルールベースの下に、いくつかのルールの説明があります。

いいえ	名前	発信元	宛先	サービス&アプリケーション	内容	アクション	追跡
規制遵守							
1	実行ファイルのダウンロードをブロック	InternalZone	インターネット	Any	トラフィック ダウンロード 実行ファイル	ドロップ	ログ 記録
2	ファイナンスのユーザによるクレジットカード番号のアップロードをHTTPSでのみ許可	ファイナンス(アクセスロール)	Web サーバ	https	トラフィック アップロード PCI - クレジットカード番号	承認	ログ 記録
3	会社のWebサーバから他のクレジットカードをブロック	InternalZone	Web サーバ	Any	任意の方向 PCI - クレジットカード番号	ドロップ ブロック メッセージ	ログ 記録
個人を特定できる情報							

いいえ	名前	発信元	宛先	サービス&アプリケーション	内容	アクション	追跡
4	米国社会保障局(SSA)により割り当てられた米国の社会保障番号(SSN)と一致します。	InternalZone	インターネット	Any	トラフィック のアップロード 米国の社会保障番号 - SSAによる	通知 Access Notifi... 1日1回 アプリごと...	ログ 記録
5	機密医療情報のダウンロードをブロック	InternalZone	インターネット	Any	トラフィック のダウンロード HIPAA - 医療記録ヘッダ	ドロップ ブロック メッセージ	ログ 記録
HR(人事)							
6	給与調査報告書を含む文書のアップロード時にユーザに確認	InternalZone	インターネット	Any	トラフィック のアップロード 給与調査レポート	確認 企業ポリシー 1日1回 アプリごと...	ログ 記録
知的財産							
7	ソースコードを含むデータとのマッチング	InternalZone	インターネット	Any	任意の方向 ソースコード	ソースコードの制限	N/A

いいえ	名前	発信元	宛先	サービス&アプリケーション	内容	アクション	追跡
7.1		Any	Any	Any	トラフィック のダウンロード ソース コード	承認	ログ 記録
7.2		Any	Any	Any	トラフィック のアップロード ソース コード	確認 企業ポリシー 1日1回 アプリごと...	ログ 記録
7.3	クリーンアップ インライン レイヤー	Any	Any	Any	Any	ドロップ ブロック メッセージ	ログ 記録

ルールについての説明：

ルール	説明
1-3	**規制遵守**セクション - 実行可能ファイルやクレジットカードのアップロードとダウンロードを制御します。 Contentの方向を設定できます。ルール1ではDownload Traffic、ルール2ではUpload Traffic、ルール3ではAny Directionです。 ルール1は、ファイルタイプである実行ファイルを制御します。ファイルタイプのルールは、コンテンツタイプのルール(ルール2 ~ 7) よりもルールベースの上位にあります。これにより、コンテンツタイプよりもファイルタイプの方が早くマッチングされるため、ルールベースの効率が向上します。
4-5	**個人識別情報**セクション - 社会保障番号や医療記録のアップロードとダウンロードを制御します。 ルール4のルールアクションはInformです。社内ユーザが社会保障番号の入ったファイルをアップロードすると、ユーザにメッセージが表示されます。
6	**人事**セクション - 給与調査情報の社外への送信を制限します。 ルールアクションはAskです。機密性の高いコンテンツが検出された場合、ユーザはそのアップロードが組織のポリシーに準拠していることを確認する必要があります。

ルール	説明
7	**知的財産**セクション - ソースコードが外部へ送られる際に制御するルールのグループ。 ルール7はインラインレイヤーの親ルール (*オーダーレイヤーとインラインレイヤー (358ページ)*)。**Action**は、インラインレイヤーの名前です。 パケットがルール7.1にマッチした場合、マッチングは停止します。 ルール7.1でパケットがマッチしない場合、ルール7.2へ進みます。同様に、一致しない場合は次の7.3へ進みます。マッチングはインラインレイヤーの最後のルールで停止します。各インラインレイヤーの最後のルールとして、明示的なクリーンアップルールを設定することをお勧めします。

使用例 - アプリケーションとURLのフィルタリング順序レイヤー

この使用例は、インターネットの閲覧をモニタおよび制御する典型的なポリシーのURLフィルタリングおよびアプリケーションコントロールルールの例です(**Hits, VPN**と**Install On**のカラムは表示されていません)。

No.	名前	発信元	宛先	サービス&アプリケーション	アクション	追跡	時間
1	賠償責任サイト	Any	インターネット	ポテンシャル負債(グループ)	ドロップ ブロック・メッセージ	ログ 記録	Any
2	ハイリスクのアプリケーション	Any	インターネット	高リスク iTunes アノニマイザー(カテゴリ)	ドロップ ブロック・メッセージ	ログ 記録	Any
3	IT部門のリモート管理を許可	IT(アクセスロール)	Any	Radmin	許可	ログ 記録	ワーク時間
4	人事部のFacebookを許可	HR(アクセスロール)	インターネット	Facebook	許可 Download_1Gbps	ログ 記録	Any

No.	名前	発信元	宛先	サービス&アプリケーション	アクション	追跡	時間
5	これらのカテゴリをブロック	Any	インターネット	ストリーミングメディアプロトコル ソーシャルネットワーク P2Pファイル共有 リモート管理	ドロップ ブロック・メッセージ	ログ記録	Any
6	すべてのアプリケーションをログ記録	Any	インターネット	Any	許可	ログ記録	Any

ルールについての説明：

ルール	説明
1	**Liability sites**- カスタム*Potential_liability*グループのサイトとアプリケーションへのトラフィックをブロックします。UserCheck*Blocked Message*はユーザに表示され、トラフィックがブロックされた理由を説明します。参照: *サイトのブロック (355ページ)*。 *シナリオ: 責任問題を引き起こす可能性のあるカテゴリに関連するサイトをブロックしたい。これらのカテゴリのほとんどはアプリケーションデータベースに存在するが、カスタム定義されたサイトも含まれなければなりません。どうすればよいですか?* *カスタムグループ*を作成し、該当するすべてのカテゴリとサイトをそのグループに追加することでこれを行うことができます。セキュリティゲートウェイで Identity Awareness を有効にすると、URL フィルタリングと一緒に使用して、*アクセスロール*に適用するルールを作成できます。アクセスロールオブジェクトを使用して、ユーザ、マシン、ネットワークロケーションを1つのオブジェクトとして定義します。 この例では ■ 以下が既に作成されています。 • 組織内のすべての識別されたユーザ(*Identified_Users*) を表すアクセスロール。 • *FreeMovies*というサイトのカスタムアプリケーション。 ■ 組織内のすべての人に責任問題を引き起こす可能性のあるサイトをブロックしたい。 ■ アプリケーションデータベースカテゴリと、以前に定義した*FreeMovies*というカスタムサイトを含むカスタムグループを作成します。 **カスタムグループを作成するには** 1. オブジェクトエクスプローラで、**New > More > Custom Application/Site > Application/Site Group**をクリックします。 2. グループに名前をつけます。例 : *Liability_Sites*。 3. **+**をクリックして、グループメンバを追加します。 ■ カスタムアプリケーション*FreeMovies*を検索し、追加します。 ■ **Categories**を選択し、ブロックしたいものを追加します (例 : *Anonymizer*、*Critical Risk*、*Gambling*) 。 ■ クリック**Close** 4. クリック**OK**。 これで、アクセスコントロールルールベースで*Liability_Sites*グループを使用できるようになります。 **ルールベースに、次のようなルールを追加します。** SmartConsoleのSecurity Policiesビューで、**Access Control Policy**にアクセスします。 ■ **Source**-**Identified_Users**アクセスロール ■ **Destination**-**Internet** ■ **Services & Applications**- *Liability_Sites*

<table>
<tr><th>ルール</th><th>説明</th></tr>
<tr><td></td><td>
Action-Drop
注 - アプリケーションは、推奨されるサービスにマッチします。各サービスは、デフォルトのApplication ControlWeb Browsing Services:<code>http,https,HTTP_proxy,HTTPS_proxy</code> のように、特定のポートで実行されます。これを変更するには、「アプリケーションとカテゴリのサービスの変更」を参照してください。
<table>
<tr><th>名前</th><th>発信元</th><th>宛先</th><th>サービス&アプリケーション</th><th>アクション</th><th>追跡</th></tr>
<tr><td>法的責任の発生する可能性のあるサイトをブロック</td><td>Identified_Users</td><td>インターネット</td><td>Liability_Sites</td><td>ドロップ</td><td>ログ記録</td></tr>
</table>
</td></tr>
<tr><td>2</td><td>High risk applications- 高リスクカテゴリのサイトやアプリケーションへのトラフィックをブロックし、iTunesアプリケーションをブロックします。UserCheck Block Messageがユーザに表示され、トラフィックがブロックされた理由を説明します。</td></tr>
<tr><td>3</td><td>Allow IT department Remote Admin- <code>IT</code>部門ネットワーク内のコンピュータがRadminアプリケーションを使用できるようにします。Radminを使用するトラフィックは勤務時間内にのみ許可されます (例 : 8:00 ~ 18:30 に設定)。</td></tr>
<tr><td>4</td><td>Allow Facebook for HR- <code>HR</code>ネットワーク内のコンピュータにFacebookの使用を許可します。Facebookからダウンロードされる総トラフィックは1Gbpsに制限され、アップロード制限はありません。</td></tr>
<tr><td>5</td><td>Block these categories- 次のカテゴリへのトラフィックをブロック: ストリーミングメディア、ソーシャルネットワーク、P2Pファイル共有、リモート管理。UserCheck Blocked Messageがユーザに表示され、トラフィックがブロックされた理由を説明します。
注 - リモート管理カテゴリは、<code>Radmin</code> アプリケーションを使用するトラフィックをブロックします。このルールをルール3の前に置くと、このルールはIT部門のRadminもブロックできます。</td></tr>
<tr><td>6</td><td>Log all applications- URLフィルタリングおよびアプリケーションコントロールのカテゴリのいずれかに一致するすべてのトラフィックをログに記録します。</td></tr>
</table>

セルフマネージド セキュリティゲート ウェイ

はじめに

R82は、高度に自動化されたネットワーク(∫) 環境を持つ顧客を支援するため、アクセスコントロールポリシーに新しいダイナミックレイヤーを導入しました。

このポリシーレイヤーは、Gaia APIコール「`set-dynamic-content`」を使用してセキュリティゲートウェイ上で直接作成されたルールのコンテナとして機能し、JSONファイルの配布を通じてプロビジョニング、コンフィギュレーション、その他のITプロセスが定期的に管理される環境に対応します。

ワークフロー:

1. 管理サーバのアクセスコントロールで、新しいポリシーレイヤーを作成し、ダイナミックレイヤーとして設定します。
2. セキュリティゲート ウェイでは、Gaia APIコール「`set-dynamic-content`」(JSON 形式) を使って、このダイナミックレイヤーに必要なアクセスコントロールルールを設定します。

ダイナミックレイヤーは、セキュリティゲート ウェイで設定したルールのコンテナとしてのみ機能します。セキュリティゲート ウェイでGaia APIコマンドを実行すると、SmartConsoleで設定されたダイナミックレイヤーのルールはすべて無視されます。永続的なルールが必要な場合 (リモート APIクライアントからのアクセスを許可する場合など) 、ダイナミックレイヤーではなく、管理サーバのメインポリシーで設定する必要があります。

詳細はsk182252を参照。

必要条件

1. 管理サーバR82以降:
   - Security Management Server
   - Multi-Domain Security Management Server
2. セキュリティゲート ウェイR82以降:
   - 単一セキュリティゲート ウェイ
   - ElasticXL Cluster
   - ClusterXL
   - Maestroまたはスケーラビリティのあるシャーシのセキュリティグループ
3. セキュリティゲート ウェイでは、Gaia APIを実行するユーザがGaia OSでこの設定を行っている必要があります:
   a. **ロール**: `adminRole`。
   b. **アクセスメカニズム**: Gaia API。
   c. **シェル**: `/bin/cli.sh or /bin/bash`

   詳細は*Gaia Administration Guide*バージョン> **ユーザ管理**の章 > **ユーザとロール**のセクション。

制限事項

- この機能はJSONフォーマット用に設計されました。

  必要なAPI本体をJSON形式で貼り付けることができる、サードパーティのREST APIクライアントを使用します。

  Check Point CLI API クライアント「`mgmt_cli`」は使用しないでください。

- セキュリティゲートウェイ上の個々の動的ルールを追加後に編集または削除することはサポートされていません。

  - 個々の動的ルールを変更するには、アクセスコントロールルール全体と、その個々のルールの更新されたパラメータと値を含む更新されたAPIボディで、Gaia APIコール "`set-dynamic-content`" を実行する必要があります。
  - 個々の動的ルールを削除するには、その個々のルールを含まない完全なアクセスコントロールルールを含む更新されたAPIボディで、Gaia APIコール "`set-dynamic-content`" を実行する必要があります。

  注:
  - 現在のルールを確認し、完全なJSONをコピーするには、セキュリティゲートウェイ上でGaia APIコール "`show-dynamic-layer`" を実行します。
  - 必要に応じて、セキュリティゲートウェイのダイナミックレイヤーにあるすべてのルールを削除できます。参照: *ダイナミックレイヤーのリセット (393ページ)*。

- VSNext Virtual Gatewayはサポートされていません。
- 従来のVSX Virtual System(VSX GatewayまたはVSX Cluster上) はサポートされていません。
- 従来の VSX バーチャル・ルータ(VSX ゲートウェイまたは VSX クラスタ上) はサポートされていない。

注

- 各 Policy Packageはインラインレイヤーまたはオーダーレイヤーとして複 数 のダイナミックレイヤーをサポート する。例 えば、管 理 者 によって異 なるPolicy Layersを使 用 することができる。
- セキュリティゲート ウェイは、ポリシーパッケージ内 のポリシーレイヤーの順 序 でアクセスコント ロールルールを適 用 します。
- ダイナミックレイヤーで設 定 したルールは、セキュリティゲート ウェイで初 めて Gaia API コール "`set-dynamic-content`" を実 行 するまで適 用 されます。
- ポリシー パッケージから動 的 レイヤを削 除 し (または動 的 レイヤのチェックボックス**Set as a Dynamic Layer**をオフにし)、アクセスコント ロールポリシーをインスト ールすると、セキュリティゲート ウェイはすべての動 的 ルールを削 除 し、SmartConsole で設 定 された静 的 ルールのみを適 用 します。
- SmartConsoleには、セキュリティゲート ウェイで設 定 したダイナミックレイヤーのルールが表 示 されません。
- ダイナミックレイヤーでサポート されているオブジェクト のリスト は、APIコール "`set-dynamic-content`" > セクション "`Request Body`" > パラメータ "`objects`" を参 照 してください。

設定

1. SmartConsoleでSecurity Management Server/Domain Management Serverにアクセスします。
2. 新しいPolicy Layerを追 加 し、Dynamic Layerとして設 定 します。

   注 :

   - 新しいPolicy Layerは、特 定 のポリシーに直 接 設 定 することも、複 数 のポリシーの共 有 Policy Layerとして設 定 することもできます。
   - インラインレイヤ(特 定 のルール内) 、またはオーダードレイヤ(専 用 のポリシーレイヤ内 の個 別 のルールセット) を設 定 できます。

     参 照 : *オーダーレイヤーとインラインレイヤー (358ページ)*。
   - 新しいポリシーレイヤーを追 加 し、ダイナミックレイヤーとして設 定 するには、SmartConsole (後 述) または管 理 API コール "`add-access-layer dynamic-layer true`" (参 照) を使 用 します(*Check Point Management API Reference*v1.8 以 降)。

   SmartConsoleの手 順 :

   特 定 のアクセスコント ロールポリシーにレイヤーを設 定 するには

   a. 左 上 隅 から、**Menu** > **Manage policies and layers**をクリックします。

   b. 左 のパネルで、**Policies**をクリックします。

c. 該当するポリシーパッケージを右クリックし、**Edit** アプリケーションをクリックします。

d. アクセスコントロールセクションで、**+**アイコンをクリックします。

e. 右上の隅で、**New Layer**をクリックします。

f. このポリシーレイヤーの名前を入力します。

g. **General** のページで次を行います。

Bladesセクションで、対応するブレードを選択します:

i. 必須:ファイアウォール

ii. オプション:アプリケーション& URLフィルタリング

h. **Advanced** のページで次を行います。

i. **Implicit Cleanup Action**セクションで、オプション「**Drop**」(デフォルト)を選択します。

このDropルールは、Gaia APIコール "`set-dynamic-content`" をセキュリティゲートウェイ上で実行するまで、このOrdered Layerにマッチするすべてのトラフィックを確実にドロップします。

後でSmartConsoleで変更できます。

ii. **Dynamic Layer**セクションで、**Set as a Dynamic Layer**を選択します。

i. **Permissions**ページで、ダイナミックレイヤーを編集できる権限プロファイルを選択します。これは、複数のダイナミックレイヤーが使用され、それぞれが異なるユーザによって設定される場合に不可欠です。ここに表示されているプロファイルだけがレイヤーを編集できます。レイヤーを編集できるプロフィールを追加するには、**Permissions**ページの下に移動します。

新しい権限プロファイルを作成するには、SmartConsoleで、[Manage & Settings] ビュー >**Permissions & Administrators** >**Permission Profiles** を開きます。プロファイルエディターで、Access Control >**Policy** と進み、**Edit layers by the selected profile in a layer editor** が選択されていることを確認します。

j. **OK** をクリックして、**Layer Editor**ウィンドウを閉じます。

k. ポリシーのアクセスコントロールセクションの右側に、**Network** (デフォルト名)というレイヤーと新しいダイナミックレイヤーが表示されます。

重要 - これらのPolicy Layersの順序を変更することができます。

l. **OK** をクリックして、**Policy** ウィンドウを閉じます。

特定のルールの特定のアクセスコントロールポリシーにインラインレイヤーを設定するには

a. 左のナビゲーションパネルから、Security Policiesをクリックします。

b. 別のセキュリティポリシーを開く必要がある場合：

   i. 上部にある [+] タブをクリックします。

   ii. 必要なポリシーをクリックします。

c. アクセスコントロールセクションで、**Policy**をクリックします。

d. 該当するルールを探します。

e. ルールで、**Action**セルをクリック > Inline Layer をクリック > **New Layer**をクリックします。

f. このポリシーレイヤーの名前を入力します。

g. **General**ページの「**Blades**」セクションで、対応するブレードを選択します：

   - 必須：ファイアウォール
   - オプション：アプリケーション& URLフィルタリング
   - オプション：**Sharing**セクションで**Multiple policies and rules can use this layer**を選択します。

h. **Advanced** のページで次を行います。

   i. **Implicit Cleanup Action**セクションでオプション**Accept**を選択します。

   これにより、セキュリティゲートウェイでGaia APIコール"`set-dynamic-content`"を実行するまで、このインラインレイヤーにマッチするトラフィックを必ず受け入れるようになります。

   後でSmartConsoleで変更できます。

   ii. **Dynamic Layer**セクションで、**Set as a Dynamic Layer**を選択します。

i. **Permissions**ページで、ダイナミックレイヤーを編集できる権限プロファイルを選択します。これは、複数のダイナミックレイヤーが使用され、それぞれが異なるユーザによって設定される場合に不可欠です。ここに表示されているプロファイルだけがレイヤーを編集できます。レイヤーを編集できるプロフィールを追加するには、**Permissions**ページの下に移動します。

   新しい権限プロファイルを作成するには、SmartConsoleで、[Manage & Settings] ビュー >**Permissions & Administrators** >**Permission Profiles** を開きます。プロファイルエディターで、Access Control >**Policy** と進み、**Edit layers by the selected profile in a layer editor** が選択されていることを確認します。

j. **OK**をクリックして**Layer Editor** ウィンドウを閉じます。

k. ルールでは、新しいインラインレイヤーが表示されています。

複数のアクセスコントロールポリシーで使用するために、共有レイヤーを設定するには

a. 左上隅から、**Menu** > **Manage policies and layers**をクリックします。

b. 左のパネルで、レイヤー > アクセスコントロールをクリックします。

c. 上部のツールバーから、**New**をクリックします。

d. このポリシーレイヤーの名前を入力します。

e. **General**ページの「**Blades**」セクションで、対応するブレードを選択します:

- 必須:ファイアウォール
- オプション:アプリケーション& URLフィルタリング
- オプション:**Sharing**セクションで**Multiple policies and rules can use this layer**を選択します。

f. **Advanced** のページで次を行います。

i. **Implicit Cleanup Action**セクションでオプション**Drop**を選択します。

このDropルールは、Gaia APIコール "`set-dynamic-content`" をセキュリティゲート ウェイ上で実行するまで、このOrdered Layerにマッチするすべてのトラフィックを確実にドロップします。

後でSmartConsoleで変更できます。

ii. **Dynamic Layer**セクションで、**Set as a Dynamic Layer**を選択します。

g. **Permissions**ページで、ダイナミックレイヤーを編集できる権限プロファイルを選択します。これは、複数のダイナミックレイヤーが使用され、それぞれが異なるユーザによって設定される場合に不可欠です。ここに表示されているプロファイルだけがレイヤーを編集できます。レイヤーを編集できるプロフィールを追加するには、**Permissions**ページの下に移動します。

新しい権限プロファイルを作成するには、SmartConsoleで、[Manage & Settings] ビュー > **Permissions & Administrators** > **Permission Profiles**を開きます。プロファイルエディタで、Access Control >**Policy** と進み、**Edit layers by the selected profile in a layer editor** が選択されていることを確認します。

h. **OK**をクリックして、**Layer Editor**ウィンドウを閉じます。

i. 左のパネルで、**Policies**をクリックします。

j. 該当するポリシーパッケージを右クリックし、**Edit**アプリケーションをクリックします。

k. アクセスコントロールセクションで、**+**アイコンをクリックします。

l. 新しいダイナミックレイヤーをクリックします。

m. ポリシーのアクセスコントロールセクションの右側に、**Network**(デフォルト名)というレイヤーと新しいダイナミックレイヤーが表示されます。

重要 - これらのPolicy Layersの順序を変更することができます。

n. **OK**をクリックして、**Policy**ウィンドウを閉じます。

o. **Close**をクリックして、**Manage policies and layers**ウィンドウを閉じます。

3. リモートAPIクライアントからセキュリティゲートウェイ上でGaia APIコールを実行する場合(セキュリティゲートウェイ上でローカルに実行しない場合)、アクセスコントロールポリシーでセキュリティゲートウェイへの接続が許可されていることを確認してください。

ベストプラクティス - APIクライアントの接続損失を回避するには、該当するルールを静的 Policy Layer (Dynamic Layer として設定されていない) にのみ追加します。

4. このアクセスコントロールポリシーをセキュリティゲートウェイ / クラスタオブジェクトにインストールします。

5. セキュリティゲートウェイ/各クラスタメンバ/セキュリティグループでGaia APIコール "`set-dynamic-content`" を実行し、必要な動的アクセスコントロールルールを設定します。

警告 - セキュリティゲートウェイで設定するルールに細心の注意を払ってください。セキュリティゲートウェイで設定されたルールとSmartConsoleで設定されたルールが競合する可能性の**検証は行われません**。

注:

- オンライン*Check Point Gaia API Reference*(v1.8以降) > セクション **System** > サブセクション**Dynamic Content**。
  ローカルのGaia APIリファレンスを参照するには、Security Management ServerまたはセキュリティゲートウェイR82以降でこのURLにアクセスします:
  ```
  https://<IP Address of Gaia Management Interface>/gaia_docs/#web/set-dynamic-content
  ```
  Gaia APIリファレンスの上部で、**Web Services**タブをクリックします。
- リモートAPIクライアントからGaia APIコールを実行するため、アクセスコントロールポリシーがセキュリティゲートウェイへの接続を許可していることを確認してください。

  ベストプラクティス - APIクライアントの接続損失を回避するには、該当するルールを静的アプリケーションPolicy Layer (Dynamic Layerとして設定されていない) にのみ追加します。

リモートREST APIクライアントのワークフロー(Postmanアプリケーションに基づく)

a. Postmanアプリケーションをインストールします。

b. sk143612からGaia REST APIコレクションを入手します。

c. Gaia REST APIコレクションをPostmanアプリケーションにインポートします(最初に、Postmanアカウントを作成することが重要です) 。インポート方法については、Postmanのドキュメントを参照してください。

d. 必要なAPI変数を設定します:

i. 左側のパネルで、Gaia REST APIコレクションの一番上のフォルダ**Gaia API**をクリックします。

ii. これらの変数を追加します:

変数名	変数値	コメント
`username`	セキュリティゲートウェイ上のGaia OSで該当するユーザのユーザ名。	デフォルトのユーザは`admin`です。 他のユーザを作成することができます(**Requirements**のセクションを参照) 。
`password`	セキュリティゲートウェイ上のGaia OSの該当ユーザのパスワード。	このパスワードを設定します。
`ip`	セキュリティゲートウェイ/各クラスタメンバ/セキュリティグループのGaia管理インタフェースのIPアドレス。	これは、APIクライアントが接続するセキュリティゲートウェイ/各クラスタメンバ/セキュリティグループのIPアドレスです。
`sid`	最初は空白です。	この変数は、Gaia APIコール"`login`"を実行した後に必要なSIDを格納するために使用するコンテナです。

e. ログインセッションID(SID) を取得します:

i. 左側のペインで、フォルダ**Session Management**を開きます。

ii. APIコール"**login**"をクリックします。

iii. 右上の隅で、**Send**をクリックします。

iv. 下のパネルで、パラメータ"**sid**"の値をコピーします。

f. SID変数を設定します:

i. 左側のパネルで、一番上のフォルダ「Gaia API」をクリックします。

ii. 変数**sid**のカラム**Current Value**にコピーした値を入力します。

iii. 右上の隅で、**Save**をクリックします。

g. セキュリティゲート ウェイ/各クラスタメンバ/Scalable Platformセキュリティグループで APIコール"`set-dynamic-content`"を実行します:

i. 左のパネルで、API "**set-dynamic-content**" をクリックします。

ii. 上部で、**Body**タブをクリックします。

iii. 必要なパラメータと値をJSON形式で設定します。

iv. 右上の隅で、**Send**をクリックします。

v. 下のパネルで、タスクIDを持つ回答全体をコピーします。

vi. 左側のパネルで**Misc**フォルダを開き、APIコール "**show task**" をクリックします。

vii. 上部で**Body**タブをクリックし、**raw**オプションをクリックします。

viii. タスクIDを含む回答全体を貼り付けます。

ix. 右上の隅で、**Send**をクリックします。

x. 下のパネルで、APIコール"`set-dynamic-content`"のAPIレスポンスを見ます。

6. **オプション**: 設定された動的アクセスコントロールルールを調べます。

- 特定のダイナミックレイヤーに設定されたダイナミックアクセスコントロールルールを見るには、セキュリティゲート ウェイ/各クラスタメンバ/セキュリティグループ上でGaia APIコール「`show-dynamic-layer`」を実行します。
- 設定されたすべてのダイナミックレイヤーで設定されたダイナミックアクセスコントロールルールを見るには、セキュリティゲート ウェイ/各クラスタメンバ/セキュリティグループでGaia APIコール「`show-dynamic-layers`」を実行します。

ダイナミックレイヤーのリセット

すべての動的ルールを削除するには、セキュリティゲート ウェイでこれらのルールを含む動的コンテナをリセットする必要があります。

手順

セキュリティゲート ウェイ上で Gaia API コール"`set-dynamic-content`" を実行し、`"operation": "reset"`を使用します。

リモートREST APIクライアントの構文部分

```
"access-layers-content": [
  {
    "name": "<Name_of_Dynamic_Layer>",
    "operation": "reset",
    "rulebase": []
  }
]
```

アクセスコントロールポリシーのインストール

重要 -「`fw up_execute`」コマンドを使用すると、アクセスコントロールポリシーを変更する前に、指定したトラフィックに対するセキュリティゲートウェイの動作(R82以上)を調べることができます。詳細は*R82 CLI Reference Guide*> "セキュリティゲートウェイコマンド"の章 > "fw"セクション > "fw up_execute"セクション。

1. グローバルツールバーで、**Menu** >**Verify Access Control Policy** > 必要なポリシーを選択 >**Verify**をクリックします。

   または、左の**Security Policies** 表示 >**Access Control** > 上のツールバーから、**Actions** >**Verify Access Policy** をクリックします。

   注 - R82からは、セッションを公開する前にアクセスコントロールポリシーを確認できます。

   必要な変更を行います。

2. 一番上のグローバルツールバーで、**Publish session**をクリックします。
3. 一番上のグローバルツールバーで、**Install Policy**をクリックします。

   Install Policyウィンドウが開き、セキュリティゲートウェイが表示されます。

4. 複数のポリシーパッケージがある場合:**Policy**ドロップダウンリストから、ポリシーパッケージを選択します。
5. **Access Control**を選択します。他のポリシーも選択可能です。
6. セキュリティゲートウェイが複数ある場合:ポリシーをインストールするセキュリティゲートウェイを選択します。
7. **Install Mode**を選択します。
   - **Install on each selected gateway independently**- 各ターゲットセキュリティゲートウェイにポリシーを独立してインストールし、いずれかのターゲットセキュリティゲートウェイでインストールに失敗しても、残りのターゲットセキュリティゲートウェイへのインストールに影響しないようにします。

     注 - **For Gateway Clusters, if installation on a cluster member fails, do not install on that cluster**を選択した場合、Security Management Serverは、インストールの開始前にすべてのクラスタメンバにポリシーをインストールできることを確認します。1つのメンバにポリシーをインストールできない場合、すべてのメンバに対してポリシーのインストールに失敗します。

   - **Install on all selected gateways, if it fails do not install on gateways of the same version**- 対象となるすべてのセキュリティゲートウェイにポリシーをインストールします。1台のセキュリティゲートウェイでポリシーのインストールに失敗した場合、他の対象のセキュリティゲートウェイにはポリシーがインストールされません。
8. クリック**Install**。

ポリシーインサイト

R82 SmartConsoleのPolicy Insights機能は、詳細なインサイトと視覚化により、管理者がポリシールールベースを分析し、最適化するのに役立ちます。Check PointのCloud Serviceは、トラフィックとポリシーを分析し、その情報に基づいてルールベースの変更を提案します。提案は内部のスケジューリングに従って生成されます。クリーンかつ効率的なルールベースで、セキュリティポリシーの管理をより容易に、さらに脆弱性を軽減します。

対応オブジェクト

ポリシー インサイトでサポートされているオブジェクト:

- ソースと宛先カラム:
  - ホスト
  - ネットワーク
  - グループ
- サービスとサービスグループ:
  - `icmp`
  - `icmp6`
  - `rpc`
  - `tcp`
  - `udp`
  - `dce-rpc`

事前準備

Security Management ServerをInfinity Portalに接続します。

参照: *SmartConsole から Infinity Portalに Security Management Server および セキュリティゲートウェイ オブジェクトを接続するには、次の手順に従います。(538ページ)*。

注 - ログ共有や設定共有を有効にする必要はありません。

ポリシーインサイトでの作業

ポリシー インサイト ウィンドウにアクセスするには

1. SmartConsoleで、セキュリティポリシービュー > アクセスコントロール > **Policy**を開きます。
2. ルールベースの上で、**Insights** ボタンをクリックします。

Policy Insightsウィンドウが開きます。

ポリシーインサイト ウィンドウのコンポーネント

ポリシー インサイト ウィンドウは3つのセクションで構成されています:

- **提案セクション**

  このセクションでは、セキュリティポリシールールベースを最適化するための実用的な推奨事項を提供します。Suggestionsセクションは、Remove unmatched objects、Replace existing objectsなどのカテゴリに分かれています。それぞれにカーソルを合わせます。

  カテゴリに基づいて提案を絞り込むことができます:

  - Show only top suggestions- セキュリティに最も影響のある提案。
  - Show suggestions (default)- 重要な提案。
  - Include low confidence suggestions- 新しいルール、最近変更されたルール、その他データが限られている場合の提案。

  各提案に対して、オプションのいずれかを選択できます:

  - Apply- ルールベースで提案された変更を行う。
  - Decline- 変更を拒否する。この提案は、Declined suggestionsセクションに移動します。
  - Decide later- 提案をDecide laterセクションに移動する。提案はその後も利用できます。

  オプションを選択したら、変更を公開し、ポリシーをインストールします。

- **後で決める セクション**

  このセクションには、もともと提案セクションにあった提案で、提案セクションに移したものが含まれます。

  To use a suggestion from the Decide laterセクション

  1. 必要な提案を選択し、Move backボタンをクリックします。
  2. Suggestionsセクションで、必要な提案を選択し、Applyをクリックします。
  3. 変更を公開しInstall Policy。

- **拒否された提案セクション**

  このセクションには、もともと提案セクションにあった提案で、Suggestionsセクションに移したものが含まれます。

Declined suggestionsセクションからの提案を使用するには

1. 必要な提案を選択し、**Undo decline**ボタンをクリックします。
2. **Suggestions**セクションで必要な提案を選択し、**Apply**をクリックします。
3. 変更を公開し、**Install Policy**。

ポリシーインサイト ウィンドウの各カテゴリでは、表示された情報が基づいている最新の日付を確認できます。

各カテゴリの数字は、そのカテゴリに対する提案の数を表しています。

各提案の横に、以下のオプションのいずれかが表示されます:

- :推奨 - セキュリティ上の影響が大きく、信頼性の高い提案。
- アイコンなし - セキュリティへの影響を示唆するものであるが、データが限られているため、決定的な信頼性はない。
- :確信度が低い - 決定的な確信を得るには十分なログと時間がない。例えば、新しいルール、最近変更されたルール、その他データが限られている場合など。

ポリシーインサイト ウィンドウの情報をCSVファイルとしてエクスポートできます。これを行うには、ポリシーインサイト ウィンドウの左下にある**Export to CSV**ボタンをクリックします。

特定のルールに関する提案を見るには

1. アクセスコントロールポリシーで、必要なルールを選択します。
2. 下のペインで、**Insights**タブをクリックします。
3. **Open**ボタンをクリックして、ポリシーインサイト ウィンドウを開きます。
4. ポリシーインサイト ウィンドウで、必要なアクションを選択します。
5. 変更を公開し、**Install Policy**。

セキュリティゲートウェイR77.30(およびそれ以下)と統合アクセスコントロールポリシー

セキュリティゲートウェイR77.30(またはそれ以下)を管理するセキュリティ管理サーバをR80.10以降にアップグレードすると、既存のアクセスコントロールポリシーが変換されます:

- **Firewall**ポリシーは**Network Policy Layer**ポリシーの**Access Control**に変換されます。適用される暗黙のクリーンアップルールは、このレイヤーのどのルールにもマッチしないすべてのトラフィックを**Drop**するように設定されます。
- **Application & URL Filtering**ポリシーは、アクセスコントロールポリシーの第2レイヤーである**Application**ポリシーの**Access Control**ポリシーレイヤーに変換されます。適用される暗黙のクリーンアップルールは、このレイヤーのどのルールにもマッチしないすべてのトラフィックを**Accept**するように設定されます。

重要 - アップグレード後は、暗黙のクリーンアップルールの**Action**や、ポリシーレイヤの順序を変更しないでください。その場合、ポリシーのインストールは失敗します。

ルールベースのヒットカウントの分析

ヒットカウントの機能を使って、各ルールがマッチした接続数を表示します。

ヒットカウントのデータを使用して:

- ルールベースの分析 - 一致する接続がないルールを削除できます。

  注 - Hit Countがゼロのルールが表示された場合は、ヒットカウントが有効になっているセキュリティゲートウェイで、一致する接続がなかったことを意味するだけです。他のセキュリティゲートウェイで一致する接続が存在する可能性があります。

- アクセスコントロールポリシーの動作の理解を深める

ヒットカウントの値は次のように表示されます。

- 合計のヒット回数に対するルールヒット数の割合
- 指標のレベル(非常に高い、高、中、低、ゼロ) 。

パーセンテージと指標のレベルは、アクセスコントロールポリシールールベースで設定されます。

ヒットカウントを有効にすると、Security Management Serverは、サポートされているセキュリティゲートウェイ(バージョンR75.40以降) からデータを収集します。

ヒットカウントはログ記録とは独立して動作し、**Track**オプションが**None**の場合でも、ヒットを追跡します。

注 - R81以降、Hit CountはNATルールベースでもサポートされています(Security Gateway R81以降が必要です) 。

ヒット数の有効化または無効化

デフォルトでは、ヒットカウントは、対応するすべてのセキュリティゲートウェイでグローバルに有効になっています。データ収集の時間範囲を定義するタイムフレーム設定は、グローバルに設定されます。必要に応じて、1つまたは複数のセキュリティゲートウェイのヒットカウントを無効にすることができます。

ヒットカウントを有効または無効にした後、データの収集を開始または停止するために、セキュリティゲートウェイのポリシーをインストールする必要があります。

ヒット数をグローバルに有効または無効にするには

1. SmartConsole で、**Menu** > **Global properties**をクリックします。
2. ツリーから**Hit Count**を選択します。
3. 以下のオプションを選択します。

- **Enable Hit Count**- 各ルールが一致した接続数をモニタするために、すべてのセキュリティゲートウェイを有効または無効にする場合はクリアを選択します。
- **Keep Hit Count data up to**- 時間範囲オプションのいずれかを選択します。デフォルトは3か月間です。データはこの期間、Security Management Serverのデータベースに保存され、ヒットカラムに表示されます。

4. クリック**OK**。
5. ポリシーをインストールします。

各セキュリティゲートウェイでヒットカウントを有効または無効にするには

1. セキュリティゲートウェイの**Gateway Properties**で、ナビゲーションツリーから**Hit Count**を選択します。
2. **Enable Hit Count**を選択して機能を有効にするか、クリアしてヒットカウントを無効にします。
3. クリック**OK**。
4. ポリシーをインストールします。

ヒットカウントの表示

ヒット数表示の設定

これらは、一致した接続データを**Hits**カラムに表示する方法について設定できるオプションです。

- **Value**- サポートされているセキュリティゲートウェイからルールに一致したヒット数が表示されます。接続回数は合計ヒット数に累積されない:
  - サポート対象外のセキュリティゲートウェイ
  - ヒットカウント機能を無効にしているセキュリティゲートウェイ

  数値はこれらの文字略号で表示されます。
  - K = 1,000
  - M = 1,000,000
  - G = 1,000,000,000
  - T = 1,000,000,000,000

  例えば、259Kは25万9千の接続を表し、2Mは200万の接続を表わします。
- **Percentage**- マッチした接続の総数に対する、そのルールのマッチしたヒット数の割合を示します。パーセンテージは10分の1を四捨五入しています。

- **Level**- ヒット数レベルは、表に従ったヒット数の範囲を示すラベルです。

  ヒット数の範囲 = 最大ヒット数-最小ヒット数(ゼロヒットは含まない)

ヒットカウントレベル	アイコン	範囲
ゼロ		0回
低		ヒット数の10%未満
中		ヒット数の10 ~ 70%の範囲
高		ヒット数の70 ~ 90%の範囲
非常に高い		ヒット数の90%以上

ルールベースのヒットカウントを表示するには

ルールベースの見出し行を右クリックし、**Hits**を選択します。

ルールのヒット数を設定するには

1. ルールのルール番号を右クリックします。
2. **Hit Count**と、オプションのいずれかを選択します(この操作を繰り返すして複数のオプションを設定できます) 。
   - **Timeframe**- 選択 : **All**,**1 day**,**7 days**,**1 month**, **3 months**
   - **Display**- 選択 : **Percentage**、**Value**、**Level**

ルールのヒット数を更新するには

1. ルールのルール番号を右クリックします。
2. **Hit Count > Refresh**を選択します。

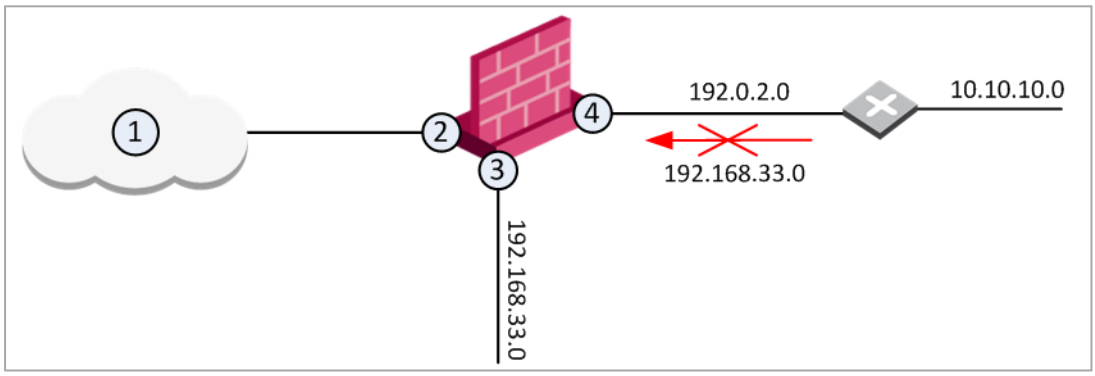
IPスプーフィングの防止

IPスプーフィングでは、信頼できない送信元IPアドレスを信頼できる偽のIPアドレスに置き換え、ネットワークへの接続を乗っ取ります。攻撃者はIPスプーフィングを利用して、保護されたネットワークにマルウェアやボットを送り込み、DoS攻撃を実行したり、不正アクセスを行ったりします。

アンチスプーフィングとは、インタフェースの背後にあるIPアドレスを持つパケットが、別のインタフェースから到着した場合に検知する機能です。例えば、外部ネットワークからのパケットが内部IPアドレスを持つ場合、アンチスプーフィングでそのパケットをブロックします。

例:

この図は、インタフェース2と3、および4を持つセキュリティゲートウェイと、その背後にあるいくつかのネットワークの例です。



セキュリティゲートウェイの場合、アンチスプーフィングは以下を確認します。

- 2への着信パケットはすべてインターネットから(1)
- 3への着信パケットはすべて`192.168.33.0`
- 4への着信パケットはすべて`192.0.2.0 or 10.10.10.0`

2への着信パケットの送信元IPアドレスがネットワーク`192.168.33.0`にある場合、送信元アドレスが偽装されているため、そのパケットはブロックされます。

Check Point Security Gatewayインタフェースにアンチスプーフィング機能を設定すると、アンチスプーフィング機能はインタフェースのトポロジに基づいて実行されます。インタフェースのトポロジは、インタフェースが**Leads To**(例えば、**外部**(インターネット)または**内部**)、およびインタフェースの**Security Zone**。

アンチスプーフィングの設定

内部インタフェースを含む、セキュリティゲートウェイのすべてのインタフェースにアンチスプーフィング保護機能を設定します。

インタフェースにアンチスプーフィングを設定するには

1. SmartConsoleの左側のナビゲーションパネルから、**Gateways & Servers**をクリックし、セキュリティゲートウェイオブジェクトをダブルクリックします。

   Gateway Propertiesウィンドウが開きます。

2. ナビゲーションツリーで、**Network Management**を選択します。

3. **Get Interfaces**をクリックします。

4. **Accept**をクリックします。

   セキュリティゲートウェイのネットワークトポロジが表示されます。SmartConsoleがトポロジを自動的に取得できない場合は、**General Properties**セクションの内容が正しいか、Security Gateway、Security Management Server、SmartConsoleが互いに通信できるかを確認します。

5. インタフェースを選択して**Edit**をクリックします。

   インタフェースのプロパティウィンドウが表示されます。

6. ナビゲーションツリーで**General**をクリックします。

7. ページの**Topology**セクションで、**Modify**をクリックします。

   Topology Settingsウィンドウが開きます。

8. **Leads To**セクションで、このインタフェースが接続するネットワークの種類を選択します。

   - **Internet (External)**- これはデフォルトの設定です。セキュリティゲートウェイのトポロジから自動的に算出されます。静的ルートの変更後に内部ネットワークのトポロジを更新するには、**Network Management**ウィンドウで**Get Interfaces** > **Gateway Properties**をクリックします。
   - **Override**- デフォルト設定を上書きします。

   デフォルト設定を**Override**(オーバーライド)する場合:

- **Internet (External)**- すべての外部/インターネットアドレス
- **This Network (Internal)**-
  - **Not Defined**- このインタフェースの背後にあるすべてのIPアドレスは、このインタフェースに接続する内部ネットワークの一部とみなされます
  - **Network defined by the interface IP and Net Mask**- この内部インタフェースに直接接続するネットワークのみ
  - **Network defined by routes**- セキュリティゲートウェイは、このインタフェースの背後にあるトポロジーを動的に計算します。このインタフェースのネットワークが変更された場合、**Get Interfaces**をクリックしてポリシーをインストールする必要はありません。詳細: *セキュリティゲートウェイトポロジの動的な更新 (231ページ)*。
  - **Specific**- この内部インタフェースの背後にある特定のオブジェクト(ネットワーク、ホスト、アドレス範囲、またはネットワークグループ)。
  - **Interface leads to DMZ**- この内部インタフェースに直接接続するDMZ

9. **オプション: Security Zone**セクションで**User defined**を選択し、**Specify Security Zone**にチェックを入れ、インタフェースのゾーンを選択します。
10. **Anti-Spoofing**オプションを設定します (*アンチスプーフィングオプション (406ページ)*)。**Perform Anti-Spoofing based on interface topology**が選択されていることを確認します。
11. **Anti-Spoofing action** を選択します。
    - **Prevent**- なりすましパケットをドロップ
    - **Detect**- なりすましパケットを許可。トラフィックを監視し、パケットをドロップせずにネットワークのトポロジを知るには、このオプションを**Spoof Tracking Log**オプションと共に選択します。
12. アンチスプーフィング例外を設定します(オプション)。例えば、アンチスプーフィングによってパケットを検査しないアドレスを設定することができます。
    a. **Don't check packets from**を選択します。
    b. ドロップダウンリストからオブジェクトを選択するか、**New**をクリックして新規オブジェクトを作成します。
13. **Spoof Tracking**を設定します。スプーフィングされたパケットが検出されたときに実行される追跡アクションを選択します。
    - **Log**- ログエントリを作成(デフォルト)
    - **Alert**- アラートを表示
    - **None**- ログやアラートを出さない
14. クリック**OK**2回押して、インタフェースのアンチスプーフィング設定を保存します。

各インタフェースについて、設定手順を繰り返します。終了したら、アクセスコントロールポリシーをインストールします。

アンチスプーフィングオプション

- **Perform Anti-Spoofing based on interface topology**- この外部インタフェースでスプーフィング保護を有効にするには、このオプションを選択します。
- **Anti-Spoofing action is set to**- パケットを拒否するか(Preventオプション) 、パケットをモニタするか(Detectオプション) を定義するには、このオプションを選択します。Detect(検出) オプションはモニタ監視するために使用されるため、いずれかの追跡オプションと組み合わせて使用する必要があります。パケットの通過を実際に妨げることなく、ネットワークのトポロジを学習するためのツールとして機能します。
- **Don't check packets from**- このオプションを選択すると、外部インタフェースに到達する内部ネットワークからのトラフィックに対してアンチスプーフィングが行われないようになります。有効なアドレスを持つ内部ネットワークを表すネットワークオブジェクトを定義し、ドロップダウンリストからそのネットワークオブジェクトを選択します。アンチスプーフィング実施メカニズムでは、**Don't check packets from**ドロップダウンメニューで選択したオブジェクトが無視されます。
- **Spoof Tracking**- 追跡オプションを選択します。

NATポリシーの設定

この章では、Check Point セキュリティゲートウェイで NAT64(IPv6からIPv4へのネットワークアドレス変換) を構成する手順について説明します。

NAT64は、IPv6のみのクライアントとIPv4のみのサーバとの通信を可能にする技術です。この構成では、IPv4/IPv6 Translation Algorithm(RFC 6145) を使用してパケットヘッダを変換するルールをCheck Pointのセキュリティゲートウェイに定義します。セキュリティゲートウェイは、N:M変換を実行し、単一のIPv4アドレスまたはアドレス範囲の背後にあるHide NATのようなシナリオをサポートします。

NATの使用

1. NATルールの種類とNATメソッドの種類については、このトピックの後述を参照してください。
2. 該当する手順に従います:
   - *自動NATルールの操作 (415ページ)*(IPv4またはIPv6変換用)
   - *Manual NATルールの操作 (425ページ)*(IPv4またはIPv6変換用)
   - *NAT46ルールの操作 (431ページ)*(IPv4からIPv6への変換用)
   - *NAT64ルールの操作 (447ページ)*(IPv6からIPv4への変換用)
3. 該当するNATの詳細設定を行います。*高度なNAT設定 (468ページ)*)。
4. アクセスコントロールポリシーをインストールします。

はじめに

NAT(Network Address Translation) は、Firewall Software Bladeの機能で、IPv4アドレスとIPv6アドレスを置き換えてセキュリティを強化するものです。NATは、ネットワークのアイデンティティを保護し、内部のIPアドレスをインターネットに表示しません。

セキュリティゲートウェイは変更できます:

- パケットの送信元IPアドレス。
- パケットの宛先IPアドレス。
- パケット内のTCP/UDPポート。

フロー例

1. 内部コンピュータが外部コンピュータにパケットを送信
2. セキュリティゲートウェイはソースIPアドレスを新しいものに変換
3. 外部コンピュータからパケットが戻る
4. セキュリティゲートウェイは新しいIPアドレスを元のIPアドレスに変換

5. 外部コンピュータからのパケットは、正しい内部コンピュータに送られます。

NATルールの種類

SmartConsoleでは、これらのタイプのNATルールを作成できます:

NATルール	NATルールの作成方法	NATルールを変更するには
自動NATルール	管理サーバは、オブジェクトのプロパティ(**NAT**ページ)で構成したNAT設定に基づいて、これらのルールを自動的に作成します。	**NAT**ページのオブジェクトのプロパティでNAT設定を変更する必要があります。
手動NATルール	これらのルールを作成し、すべてのオブジェクトとNATメソッドを選択します。	これらのルールを変更します。

重要 - Security Management Server/Domain Management Serverは、1つのポリシーで最大16384のNATルールをサポートします。See sk82220

NAT方式の種類

自動NATルールおよび手動NATルールでは、これらのNAT方法のいずれかを設定できます:

非表示にする

セキュリティゲートウェイは、送信元からのすべての接続の送信元IPアドレスを、セキュリティゲートウェイの送信インタフェースのIPアドレス、または設定したIPアドレスと同じIPアドレスに変更します。

隠す > ゲートウェイ背後に隠す

セキュリティゲートウェイは、送信元からのすべての接続の送信元IPアドレスを、セキュリティゲートウェイの送信インタフェースの同じIPアドレスに変更します。

隠す > IPアドレスで隠す

セキュリティゲートウェイは、送信元からのすべての接続の送信元IPアドレスを、設定したのと同じIPアドレスに変更します。

注:

- Hide NATを設定すると、内部コンピュータからのみ接続を開始できるようになります。
  セキュリティゲートウェイは、外部トラフィックが内部リソースにアクセスすることを許**可しません**。
- 1つのIPアドレスを表すオブジェクト(Hostオブジェクト)でこの設定を有効にすると、1対1のアドレス変換が行われます。
- 多くのIPアドレスを表すオブジェクト(Networkオブジェクト、Address Rangeオブジェクト)でこの設定を有効にすると、多対一のアドレス変換が行われます。
- セキュリティゲートウェイは、ポート番号を使用して、指定されたすべての内部IPアドレスを1つの外部IPアドレスに変換します(ポート番号は600 ~ 1023、10,000 ~ 60,000)。
  セキュリティゲートウェイは、同時に最大50,000の接続を変換できます。
- 次の構成には、Hide NATは使用できません。
  - ポート番号を変更できないプロトコルを使用するトラフィック。
  - IPアドレスを使用して異なるコンピュータやクライアントを識別する外部サーバ。

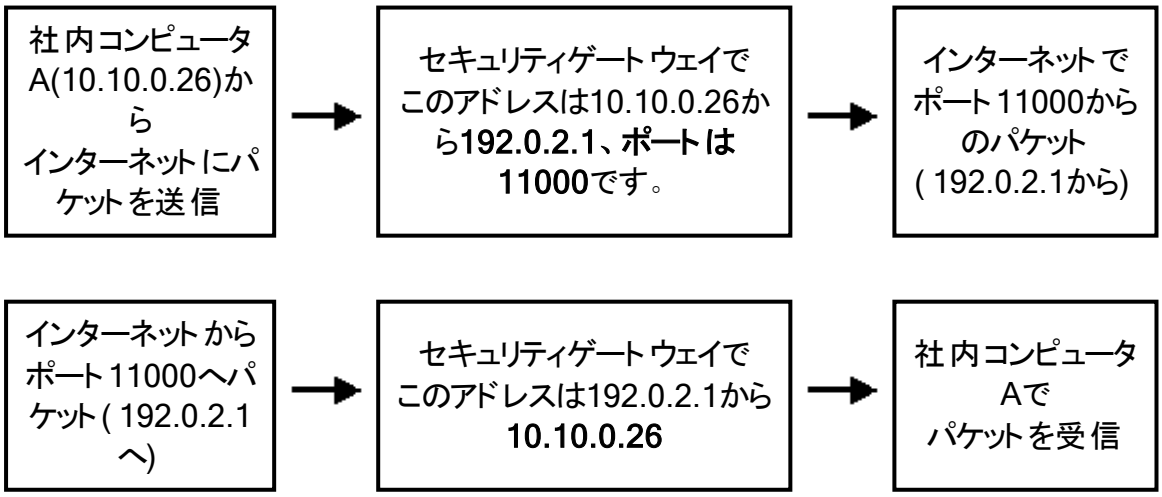
ダイアグラムの例



項目	説明
1	社内コンピュータ
2	Hide NATで構成されたセキュリティゲートウェイ
3	インターネット上の外部のコンピュータやサーバ

Hide NATワークフローの例

1. 内部コンピュータA(10.10.0.26) から外部コンピュータにパケットが送信されます。
2. セキュリティゲートウェイはパケットを阻止し、ソースIPアドレスを(10.10.0.26)から192.0.2.1に、ポートを11000に変換します。
3. 外部コンピュータは192.0.2.1へ、ポート11000にパケットを送り返します。
4. セキュリティゲートウェイはパケットのIPアドレスを192.0.2.1から10.10.0.26に変換し、内部コンピュータAに送信します。



スタティック

セキュリティゲートウェイは、ソースからのすべての接続のソースIPアドレスを設定したIPアドレスに変更します。

注:

- スタティックNATを設定すると、セキュリティゲートウェイは外部トラフィックが内部リソースにアクセスできるようになります。
- 1つのIPアドレスを表すオブジェクト(Hostオブジェクト)でこの設定を有効にすると、1対1のアドレス変換が行われます。
- 多くのIPアドレスを表すオブジェクト(Networkオブジェクト、Address Rangeオブジェクト)でこの設定を有効にすると、多対一のアドレス変換が行われます。セキュリティゲートウェイは、それぞれの内部IPアドレスを異なる外部IPアドレスに変換します。

  重要 - 変換されたIPアドレスの範囲は、ソースIPアドレスの範囲と同じです。

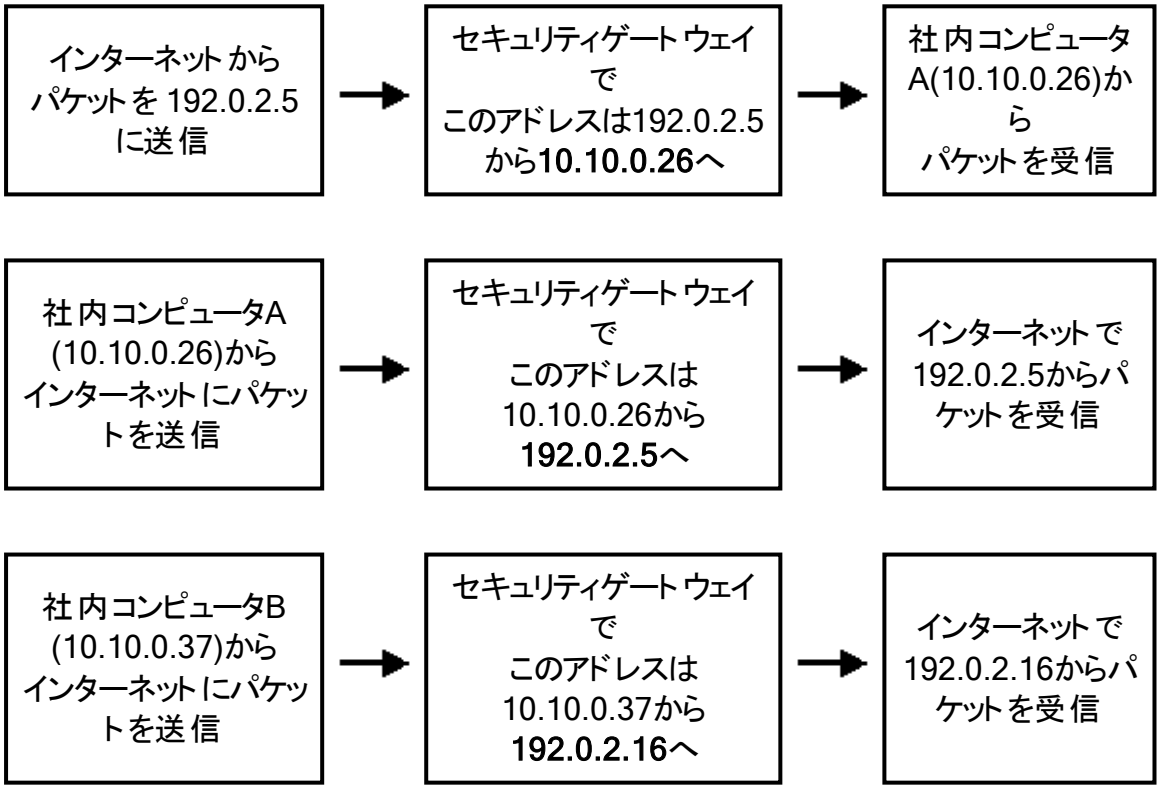
ダイアグラムの例



項目	説明
1	社内コンピュータ
2	静的NATで構成されたセキュリティゲートウェイ
3	インターネット上の外部のコンピュータやサーバ

スタティックNATによるトラフィックフローの例

1. インターネット上の外部コンピュータが192.0.2.5にパケットを送信。
2. セキュリティゲートウェイはIPアドレスを192.0.2.5から10.10.0.26に変換し、パケットを内部コンピュータAに送信。
3. 内部コンピュータA(10.10.0.26) は外部コンピュータにパケットを送り返す。
4. セキュリティゲートウェイはパケットをインターセプトし、ソースIPアドレスを10.10.0.26から192.0.2.5に変換。
5. 内部コンピュータB(10.10.0.37) から外部コンピュータにパケットが送信されます。
6. セキュリティゲートウェイはパケットを阻止し、ソースIPアドレスを10.10.0.37から192.0.2.16に変換。



SmartConsoleのNATルール

NATルールベースには2つのセクションがあり、IPアドレスとポートの変換方法を指定します:

- **Original**- カラム**Source**、**Destination**、および**Services**
- **Translated**- カラム**Source**、**Destination**、および**Services**

自動NATルールの例

いいえ	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
自動生成ルール								
XのNATルール(Y-Z)								
1	オブジェクト1	オブジェクト2	Any	= Original	= Original	= Original	Policy Targets	
2	オブジェクト3	オブジェクト4	Any	Sオブジェクト5	Sオブジェクト6	= Original	Policy Targets	
3	オブジェクト7	オブジェクト8	Any	Hオブジェクト9	Hオブジェクト10	= Original	Policy Targets	

手動NATルールの例

いいえ	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
自動生成ルール								
手動ルール(低)								
4	オブジェクト11	オブジェクト12	Any	Sオブジェクト13	= Original	= Original	Policy Targets	
5	オブジェクト14	オブジェクト15	Any	= Original	Sオブジェクト16	= Original	Policy Targets	

NATルール実施の順番

セキュリティゲートウェイは、NATポリシーでルールを配置した順番に、NATルールベースを実施します(**No.**カラムを参照) 。

セキュリティゲートウェイは、自動NATルールと手動NATルールを異なる方法で実施します。

説明

- **Manual NAT rules**- セキュリティゲートウェイは、接続にマッチした最初の手動NATルールを実施します。セキュリティゲートウェイは他の手動NATルールを検査しません。
- **Automatic NAT rules**- セキュリティゲートウェイは、接続にマッチする2つの自動NATルール(1つは**Source** 、もう1つは**Destination**) を強制できます。接続が2つの自動NATルールにー致すると、セキュリティゲートウェイはそれらのルールを実施します。

  注 - SmartConsoleは、自動NATルールをこの順序で整理します:
  1. セキュリティゲートウェイ、またはホスト(コンピュータまたはサーバ) オブジェクトの静的NATルール
  2. セキュリティゲートウェイ、またはホストオブジェクトのHide NATルールを隠す
  3. ネットワークまたはアドレスレンジオブジェクトの静的NATルール
  4. ネットワークまたはアドレスレンジオブジェクトのHide NATルールを隠す

自動NATルールの操作

これらのオブジェクトに自動NATルールを作成できます:

- セキュリティゲートウェイ
- ホスト
- ネットワーク
- アドレス範囲

管理サーバは、パケットのソースと宛先を変換するために、スタティックNAT用に2つの自動NATルールを作成します。

Hide NATでは、1つのルールがパケットのソースを変換します。

NetworkオブジェクトとAddress Rangeオブジェクトの場合、管理サーバはイントラネットトラフィックを変換しない別のルールを作成します。同一オブジェクト上のコンピュータのIPアドレスは変換されません。

この表は自動NATルールをまとめたものです:

トラフィックのタイプ	自動NAT - スタティック	自動NAT - Hide NAT
内部から外部	ルールは、ソースIPアドレスを変換	ルールは、ソースIPアドレスを変換
外部から内部	ルールは、宛先IPアドレスを変換	N/A (外部接続不可)
イントラネット (ネットワークとアドレス範囲オブジェクト)	ルールでIPアドレスを変換しない	ルールでIPアドレスを変換しない

自動NATルールの例

ネットワークオブジェクトのスタティックNAT

いいえ	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
自動生成ルール								
HRのNATルール (1-3)								
1	HR	HR	Any	= Original	= Original	= Original	Policy Targets	

いいえ	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
2	HR	Any	Any	SHR(有効アドレス)	= Original	= Original	Policy Targets	
3	Any	HR(有効アドレス)	Any	= Original	SHR	= Original	Policy Targets	

1. HRネットワークのイントラネット接続は変換されません。

   セキュリティゲートウェイは、HRオブジェクトの一部である2台のコンピュータ間の接続を変換しません。

   セキュリティゲートウェイは、ルール1に一致するトラフィックにはルール2と3を適用しません。

2. HRネットワークからのIPアドレスから任意のIPアドレス(通常は外部のコンピュータ)への接続は、Static NATのIPアドレスに変換されます。

3. 任意のIPアドレス(通常は外部のコンピュータ)からHRへの接続は、Static NATのIPアドレスに変換されます。

Address Rangeオブジェクトのhide NAT

いいえ	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
自動生成ルール								
SalesのNATルール(1-2)								
1	Sales	Sales	Any	= Original	= Original	= Original	Policy Targets	
2	Sales	Any	Any	HSales(アドレス非表示)	= Original	= Original	Policy Targets	

1. Salesアドレスの範囲内のイントラネット接続は変換されません。

   ファイアウォールは、Salesオブジェクトに含まれるIPアドレスを使用する2つのコンピュータ間の接続を変換しません。

   ファイアウォールは、ルール1に一致するトラフィックにルール2を適用しません。

2. Salesアドレスの範囲にあるIPアドレスから任意のIPアドレス(通常は外部のコンピュータ)への接続は、Hide NATのIPアドレスに変換されます。

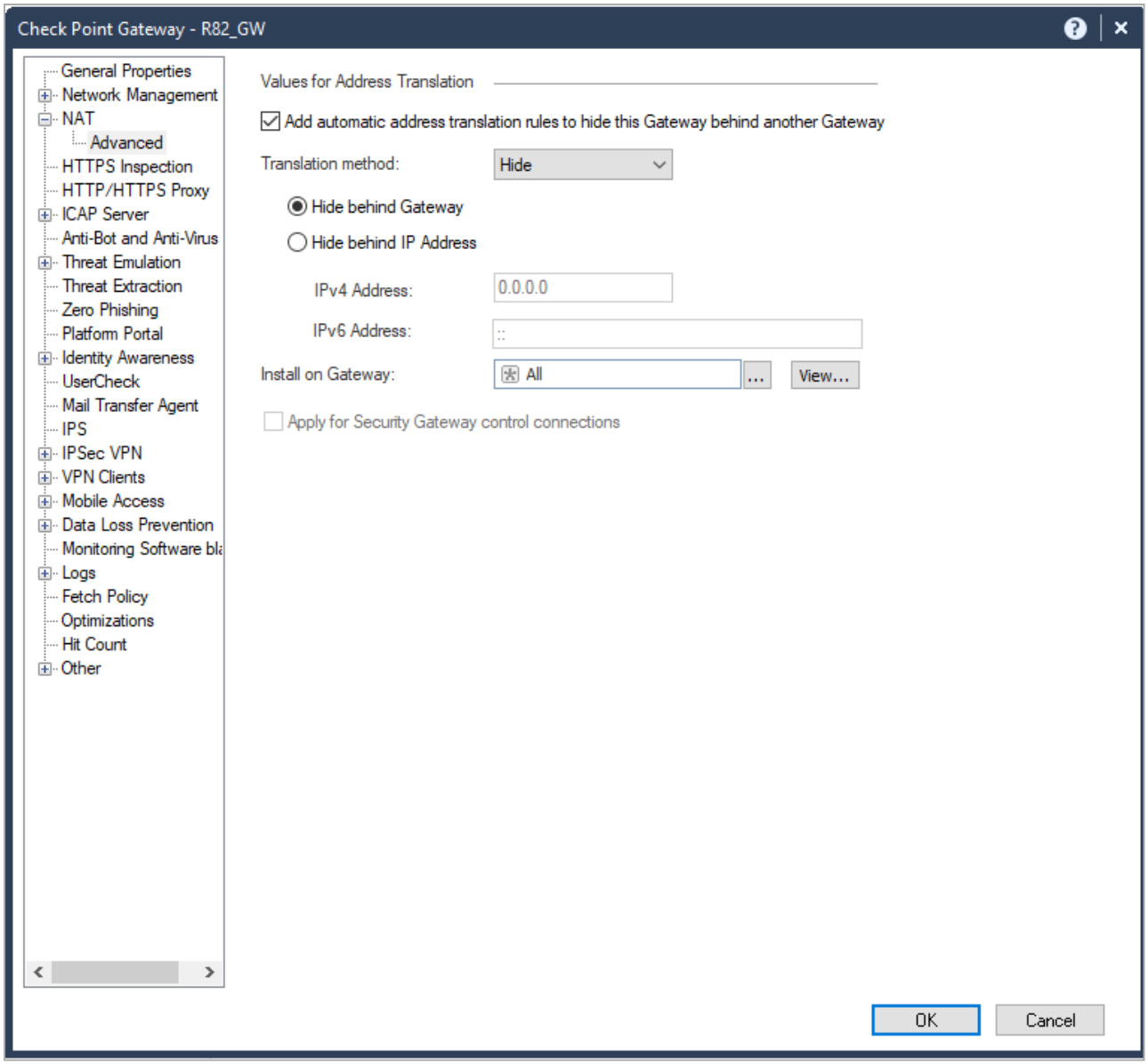
自動NATの設定

自動NATルールを作成する必要がある各オブジェクトでNAT設定を構成し、該当するオブジェクトへのトラフィックを許可するようにアクセスコントロールルールを設定します。

手順

1. 左側のナビゲーションパネルで**Gateways & Servers**をクリックします。
2. Security Gatewayオブジェクトを右クリックします。

   ゲートウェイの**General Properties**ウィンドウが開きます。
3. ナビゲーションツリーから、**NAT >Advanced** を選択します。
4. **Add automatic address translation rules to hide this Gateway behind another Gateway**を選択します。
5. **Translation method**:**Hide**または**Static**を選択します。
6. オブジェクトのNAT IPアドレスを設定します。
   - **Hide behind Gateway**- 対応するセキュリティゲートウェイのインタフェースのIPアドレスを使用。
   - **Hide behind IP address**- IPアドレスを入力。
7. **Install on Gateway**をクリックし、**All**またはIPアドレスを変換するセキュリティゲートウェイを選択します。
8. OKをクリックします。
9. アクセスコントロールポリシーをインストールします。



デプロイメント例

例

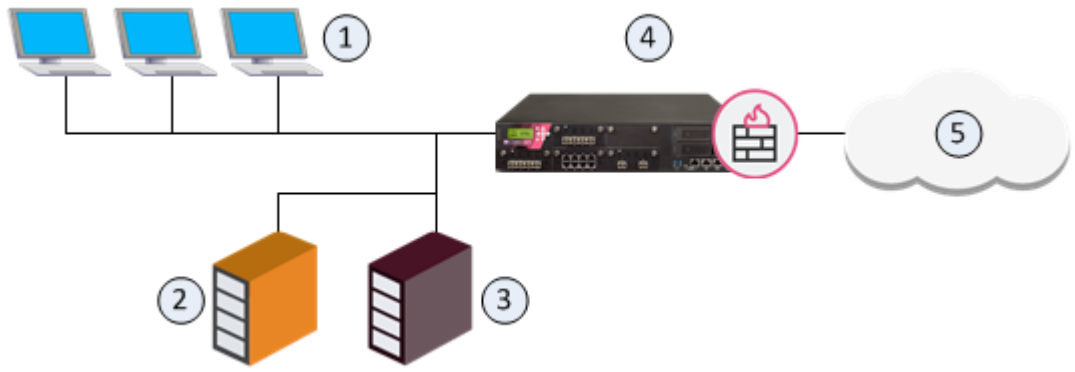
この導入サンプルの目的は、次を設定することです。

- 内部ネットワーク上のメールサーバとWebサーバのスタティックNAT。

  これらのサーバは、インターネットからパブリックアドレスを使ってアクセスできます。

- インターネットにアクセスする内部ネットワークのユーザに対するHide NAT。

  このネットワークは、インターネットからアクセスすることはできません。



項目	説明
1	内部コンピュータ(**Alaska_LAN**、IPv6 2001:db8::/64)
2	Webサーバ(**Alaska_Web**、IPv6 2001:db8:0:10::5はIPv6 2001:db8:0:a::5に変換)
3	メールサーバ(**Alaska_Mail**、IPv6 2001:db8:0:10::6はIPv6 2001:db8:0:a::6に変換)
4	セキュリティゲートウェイ(**Alaska_GW**、外部IPv6 2001:db8:0:a::1)
5	インターネット上の外部のコンピュータやサーバ

設定手順:

1. Webサーバに自動静的NATを設定:
    a. **Alaska_Web**オブジェクトをダブルクリックします。
    b. 左から**NAT**をクリックします。
    c. **Add Automatic Address Translation Rules**を選択します。
    d. **Translation method**で、**Static**を選択します。
    e. **Hide behind IP Address**を選択し、**2001:db8:0:a::5**を入力します。
    f. クリック**OK**
2. EMailサーバの自動静的NATを有効化:
    a. **Alaska_Mail**オブジェクトをダブルクリックします。
    b. 左から**NAT**をクリックします。
    c. **Add Automatic Address Translation Rules**を選択します。
    d. **Translation method**で、**Static**を選択します。

e. **Hide behind IP Address**を選択し、**2001:db8:0:a::6**を入力します。

f. クリック**OK**。

3. 内部コンピュータの自動Hide NATを有効化：

a. **Alaska_LAN**オブジェクトをダブルクリックします。

b. 左から**NAT**をクリックします。

c. **Add Automatic Address Translation Rules**を選択します。

d. **Translation method**で、**Hide**を選択します。

e. **Hide behind Gateway**を選択します。

4. クリック**OK**。

5. アクセスコントロールポリシーをインストールします。

管理サーバは、**Security Policies**ビュー>**Access Control**>**NAT**で、これらの自動NATルールを作成します：

いいえ	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
自動生成ルール								
SalesのNATルール(1-2)								
1	Alaska_Web	Alaska_Web	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_Web	Any	Any	S Alaska_Web(有効なアドレス)	= Original	= Original	Policy Targets	
3	Any	Alaska_Web	Any	= Original	S Alaska_Web(有効なアドレス)	= Original	Policy Targets	
4	Alaska_Mail	Alaska_Mail	Any	= Original	= Original	= Original	Policy Targets	

いいえ	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
5	Alaska_Mail	Any	Any	S Alaska_Mail(有効なアドレス)	= Original	= Original	Policy Targets	
6	Any	Alaska_Mail	Any	= Original	S Alaska_Mail(有効なアドレス)	= Original	Policy Targets	
7	Alaska_LAN	Alaska_LAN	Any	= Original	= Original	= Original	Policy Targets	
8	Alaska_LAN	Any	Any	H Alaska_LAN (非表示アドレス)	= Original	= Original	Policy Targets	

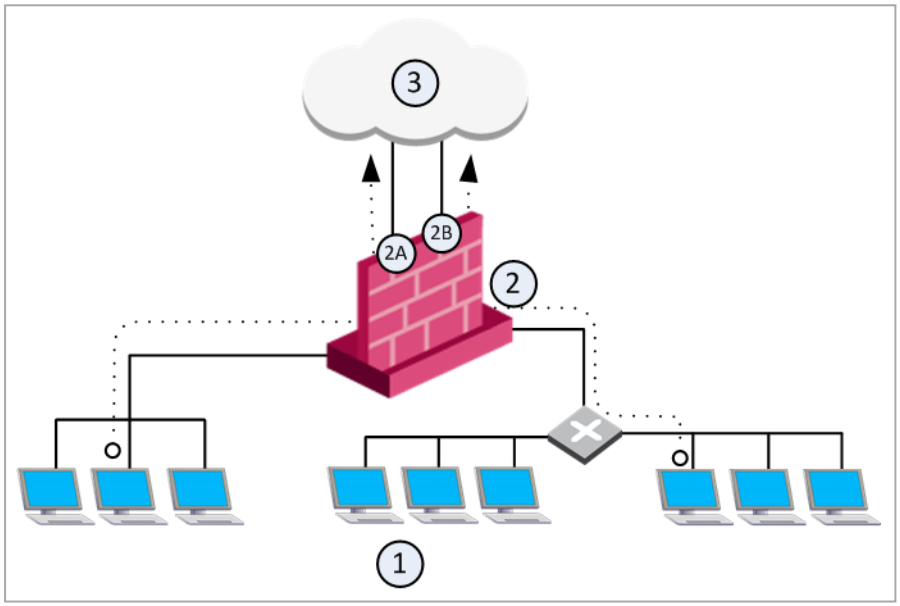
外部ネットワークへの自動Hide NAT

大規模で複雑なネットワークの場合、すべての内部IPアドレスに対してHide NATの設定を行うことは実用的でない場合があります。

説明

簡単な代替方法は、セキュリティゲートウェイを有効にして、外部ネットワークとのすべてのトラフィックに対して自動的にHide NATを行うことです。セキュリティゲートウェイは、外部インタフェースを経由するすべてのトラフィックを、そのインタフェースの有効なIPアドレスに変換します。

このサンプルでは、内部ネットワークのコンピュータがインターネット上の外部サーバへの接続を開く構成になっています。内部クライアントの発信元IPアドレスは、外部インタフェースのIPアドレスに変換されます。



項目	説明
1	社内ネットワーク
2	セキュリティゲートウェイは自動Hide NATで設定されています。
2A、2B	外部インタフェース 192.0.2.1 と 192.0.2.100 の2つ。
1 -->3	インターネット上の外部のコンピュータやサーバ

ソースIPアドレスは、該当する外部インタフェースIPアドレスに変換されます: **192.0.2.1**または**192.0.2.100**。

注 - 接続が通常のNATルールとNAT-for-Internal-Networksルールに一致する場合、通常のNATルールが優先されます。

自動Hide NATを有効にするには

1. 左側のナビゲーションパネルで**Gateways & Servers**をクリックします。
2. Security Gatewayオブジェクトを右クリックします。
3. ナビゲーションツリーで**NAT**をクリックします。
4. **Hide internal networks behind the Gateway's external IP**を選択します。
5. クリック**OK**。
6. アクセスコントロールポリシーをインストールします。

Manual NATルールの操作

一部の導入では、NATルールを手動で定義する必要があります。

例:

- 特定の宛先IPアドレスと特定の送信元IPアドレスに制限されたルール
- 同一パケット内でソースIPアドレスと宛先IPアドレスの両方を変換。
- 片方向のみの静的NAT
- 変換サービス(宛先ポート)
- 指定したサービス(ポート)のみを利用するルール
- 動的オブジェクトのIPアドレスの変換

手動NATルールを使用する場合の一般的なワークフロー:

1. **valid** (NATed) IPアドレスを使用するSmartConsoleオブジェクトを作成します。
2. 手動NATルールを作成し、オブジェクトの元のIPアドレスを有効なIPアドレスに変換します。
3. 有効なIPアドレスを持つ該当する変換オブジェクトへのトラフィックを許可するように、アクセスコントロールポリシーを設定します。

注 - 手動NATルールの場合、変換されたIPアドレスを関連付けるためにプロキシARPエントリを設定する必要があります。参照: *自動およびプロキシ ARP (468ページ)*。

手動NATルールの例

いいえ	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
1	HTTP_Client	Web_Server	http	= Original	S Web_Server	= Original	Policy Targets	

手動NATの設定

手順

1. 左のナビゲーションツリーから、Security Policiesをクリックします。
2. **Access Control >NAT** をクリックします:
3. 以下のいずれかの方法で新しいルールを追加します:
   - 一番上のツールバーから、**Add Rule**アイコン(一番左のアイコン)をクリックします。
   - 既存の手動NATルールがある場合は、該当するルールの**No.** カラムで右クリックし、**New Rule**行で、**Above**または**Below**をクリックします。
4. 新しいルールで必要なオブジェクトを選択し、必要な変換を設定します。

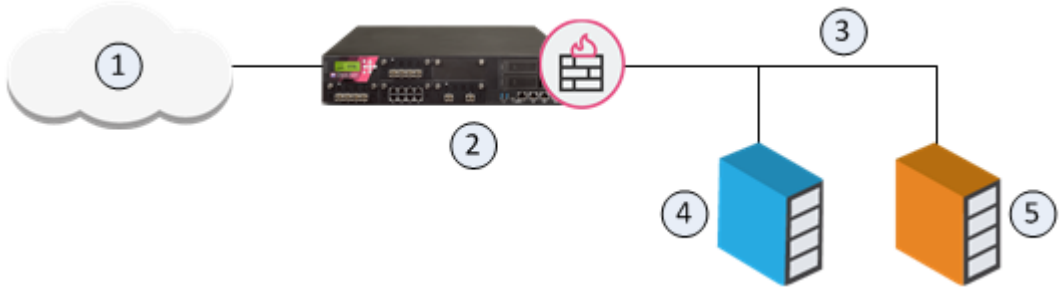
   必要なオブジェクトが存在しない場合は、選択ウィンドウで作成することができます(右上隅で**New**をクリック)。
5. アクセスコントロールポリシーをインストールします。

デプロイメント例

例

この設定例では、DMZネットワーク内の内部Webサーバと内部メールサーバに、外部コンピュータが1つのIPアドレスからアクセスできるようにする方法を示しています。

これを行うには、DMZネットワークオブジェクトにHide NATを設定し、サーバ用に手動NATルールを作成する必要があります。



項目	説明
1	インターネット上の外部のコンピュータやサーバ
2	セキュリティゲートウェイ(**Alaska_GW**、外部IPv6 2001:db8:0:c::1)
3	DMZネットワーク(**Alaska_DMZ**、IPv6 2001:db8:a::/128)

項目	説明
4	Webサーバ(**Alaska_DMZ_Web**、IPv6 2001:db8:a::35:5はIPv6 2001:db8:0:c::1に変換)
5	メールサーバ(**Alaska_DMZ_Mail**、IPv6 2001:db8:a::35:6はIPv6 2001:db8:0:c::1に変換)

設定手順:

1. DMZネットワークに自動Hide NATを設定:
   a. ネットワークオブジェクト **Alaska_DMZ**をダブルクリックします。
   b. 左から**NAT**をクリックします。
   c. **Add Automatic Address Translation Rules**を選択します。
   d. **Translation method**で、**Hide**を選択します。
   e. **Hide behind Gateway**を選択します。
   f. クリック**OK**。

   管理サーバは、[Security Policies] ビュー >**Access Control** >**NAT** で、これらの自動NATルールを作成します:

No.	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (アドレス非表示)	= Original	= Original	Policy Targets	

2. 受信HTTPトラフィックを内部Webサーバに変換する手動NATルールを作成:

a. SmartConsoleで、Security Policies view >**Access Control** >**NAT** を開きます。

b. 既存の自動NATルールの下に新しいルール(#3) を追加します。

c. これらのオブジェクトを選択します:

No.	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (アドレス非表示)	= Original	= Original	Policy Targets	
3	Any	Alaska_GW	http	= Original	S Alaska_DMZ_Web	= Original	Policy Targets	

3. 受信SMTPトラフィックを内部メールサーバに変換する手動NATルールを作成します:

a. 既存のNATルールの下に新しいルール(#4) を追加します。

b. これらのオブジェクトを選択します:

No.	元のソース	元の宛先	元のサービス	変換ソース	変換宛先	変換サービス	インストール先	コメント
1	Alaska_DMZ	Alaska_DMZ	Any	= Original	= Original	= Original	Policy Targets	
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (アドレス非表示)	= Original	= Original	Policy Targets	
3	Any	Alaska_GW	http	= Original	S Alaska_DMZ_Web	= Original	Policy Targets	
4	Any	Alaska_GW	smtp	= Original	S Alaska_DMZ_Mail	= Original	Policy Targets	

4. 内部サーバへのHTTPおよびSMTPトラフィックの着信を許可するアクセスコントロールルールを作成します:

a. SmartConsoleで、Security Policies >**Access Control** >**NAT** と進みます。

b. 3. 新しいルールを追加します。

c. これらのオブジェクトを選択します:

いいえ	名前	発信元	宛先	VPN	サービス&アプリケーション	アクション	追跡	インストール先
...	内部サーバへのHTTPおよびSMTPトラフィックの着信	Any	Alaska_DMZ	Any	http smtp	Accept	Log	Policy Targets

5. アクセスコントロールポリシーをインストールします。

NAT46ルールの操作

注 - NAT46ルールは、セキュリティゲートウェイおよびクラスタメンバR80.20以降でのみサポートされています。

メニュー

NAT46ルールは、セキュリティゲートウェイ上のセッション情報を維持することなく、IPv4トラフィックをIPv6トラフィックに変換します。

ステートレスNAT46のプロパティ

- 1:1のIPアドレスマッピングを行います。
- システムは、これら2つのパーツの組み合わせとして、変換されたソースIPv6アドレスを生成します。
  1. 96ビットのプレフィックスで定義されたIPv6アドレスを持つユーザ定義のNetworkオブジェクト。
  2. 送信元のIPv4アドレスで、32ビットのサフィックスとして付加されます。

NAT46の使用シナリオ

- [IPv4ネットワーク] --- (インターネット) --- [セキュリティゲートウェイ] --- [IPv6ネットワーク]

  コンテンツプロバイダの一般的な使用例。
- [IPv4ネットワーク] --- [セキュリティゲートウェイ] --- (インターネット) --- [IPv6ネットワーク]

  企業における一般的な使用例。

NAT46変換フロー例

トポロジの例:

[IPv4クライアント] ---(内部) [セキュリティゲートウェイ] ---(外部) [IPv6 サーバ]

各変数の意味は以下のとおりです。

項目	説明
IPv4クライアント	IPv4実アドレスは192.168.2.55です。 IPv6 NATed アドレスは2001:DB8:90::192.168.2.55/**96**です。
セキュリティゲートウェイ 内部インタフェース	IPv4アドレスは192.168.2.1/24です。
セキュリティゲートウェイ 外部インタフェース	IPv6アドレスは2001:DB8:5001::1/**96**です。

項目	説明
IPv6サーバ	IPv6実アドレスは2001:DB8:5001::30/96です。 IPv4 NATed アドレスは 1.1.1.66/24 です。
IPv6 NATedネットワーク	外部Security Gateway側のネットワークのIPv6アドレスは2001:DB8:90::/96です。 これらのIPv6アドレスは、IPv4クライアントのIPv4アドレスをIPv6アドレスに変換するために使用されます。
IPv4 NATedネットワーク	内部Security Gateway側のネットワークのIPv4アドレスは1.1.1.0/24です。 これらのIPv4アドレスは、IPv6サーバのIPv6アドレスをIPv4アドレスに変換するために使用されます

トラフィックフロー:

1. IPv4クライアントは、IPv6サーバのNATed IPv4アドレスにIPv4接続を開始します。

   IPv4アドレス 192.168.2.55 から IPv4アドレス 1.1.1.66へ

2. Security Gatewayは、これらのNAT変換を実行します。

   a. 送信元IPv4アドレス192.168.2.55から送信元IPv6アドレス2001:DB8:90::192.168.2.55/96へ

   b. 宛先IPv4アドレス1.1.1.66から宛先IPv6アドレス2001:DB8:5001::30へ

3. IPv6サーバは、このリクエスト接続をIPv6アドレス 2001:DB8:90::192.168.2.55/96からIPv6アドレス 2001:DB8:5001::30 として受け取ります。

4. IPv6サーバはこの接続に対して、IPv6アドレス2001:DB8:5001::30からIPv6アドレス2001:DB8:90::192.168.2.55/96まで返信します。

5. Security Gatewayは、これらのNAT変換を実行します。

   a. 送信元IPv6アドレス2001:DB8:5001::30から送信元IPv4アドレス1.1.1.66へ

   b. 宛先IPv6アドレス 2001:DB8:90::192.168.2.55/96 から宛先IPv4アドレス192.168.2.55へ

6. IPv4クライアントは、この応答接続を IPv4アドレス 1.1.1.66 から IPv4 アドレス 192.168.2.55までとして受信します。

要約すると

- リクエスト: [IPv4クライアント] ---> [セキュリティゲートウェイ] ---> [IPv6サーバ]

パケット内のフィールド	元のIPv4パケット	NATed IPv6パケット
ソースIP	192.168.2.55 / 24	2001:DB8:90::192.168.2.55 / 96
宛先IP	1.1.1.66 / 24	2001:DB8:5001::30 / 96

- 返信: [IPv4クライアント] <--- [セキュリティゲートウェイ] <--- [IPv6サーバ]

パケット内のフィールド	元のIPv6パケット	NATed IPv4パケット
ソースIP	2001:DB8:5001::30 / 96	192.168.2.55 / 24
宛先IP	2001:DB8:90::192.168.2.55 / 96	1.1.1.66 / 24

NAT46の既知の制限事項

- NAT46ルールは、Security GatewayおよびクラスタメンバのR80.20以降でのみサポートされます。
- NAT46はVoIPトラフィックをサポートしません。
- NAT46はFTPトラフィックをサポートしません。
- NAT46は、コントロール接続とデータ接続の間に状態情報を必要とするプロトコルをサポートしません。

NAT46の設定

ステップ1 - NAT46用のセキュリティゲートウェイ/クラスタメンバの準備

注 -クラスタでは、すべてのクラスタメンバを同じ方法で設定する必要があります。

ステップ	手順
1	宛先IPv6ネットワークに接続するインタフェースにIPv6アドレスが割り当てられ、IPv6ネットワークプレフィックス長が96に等しいことを確認してください。 **注** - これは、IPv6ネットワークプレフィックス長が**96**である有効なIPv6アドレスであれば、どれでもかまいません。 ■ Gaia Portal: **Network Management > Network Interfaces**をクリックします。 ■ Gaia Clish: 次を実行します: `show interface <Name of Interface> ipv6-address` IPv6アドレスが割り当てられていない場合は、今すぐ割り当ててください。 詳細:*R82 Gaia Administration Guide- ネットワーク管理章 - セクション ネットワークインタフェース - セクション 物理インタフェース*

ステップ	手順

2	NATされたIPv4アドレス(NAT46ルールの*Translated Destination*カラムに定義されている) 宛てのトラフィックを、宛先IPv6ネットワークに接続するインタフェース経由で送信するようにルーティングが設定されていることを確認します。
	■ Gaia Portal:
	Advanced Routing > Routing Monitorをクリックします。
	■ Gaia Clish:
	次を実行します:
	`show route`
	もし、そのようなルートがまだ存在しない場合は、Gaia Clishで追加してください。
	詳細 : *R82 Gaia Administration Guide*。
	これらのコマンドをGaiaClishで実行します。
	1. スタティックルートを追加します。
	`set static route <NATed Destination IPv4 Addresses>/<NATed IPv4 Net Mask> nexthop gateway logical <Name of Interface that connects to the real IPv6 Network> on`
	トポロジの例:
	[IPv4クライアント] --- (IPv6側のNATed IPv4は1.1.1.0/24) [セキュリティゲートウェイ] (eth3) --- [IPv6サーバ]
	この場合、次のコマンドでIPv4ルートを設定します。
	`set static route 1.1.1.0/24 nexthop gateway logical eth3 on`
	2. 設定を保存します。
	`save config`

ステップ	手順

3	IPv6 CoreXL Firewallインスタンスの数が、IPv4 CoreXL Firewallインスタンスの数と**同じ**であることを確認します。
	1. Security Groupでコマンドラインに接続します。
	2. Gaia Clish、またはエキスパートモードにログインします。
	3. IPv6 CoreXL Firewallインスタンスの数を表示します。
	`fw6 ctl multik stat`
	4. IPv4 CoreXL Firewallインスタンスの数を表示します。次を実行します:
	`fw ctl multik stat`
	5. IPv6 CoreXL Firewallインスタンスの数がIPv4 CoreXL Firewallインスタンスの数より少ない場合、次の手順を実行します。
	a. 次を実行します:
	`cpconfig`
	b. 選択**Check Point CoreXL**
	c. 選択**Change the number of IPv6 firewall instances**
	d. IPv6 CoreXL Firewallインスタンスの数をIPv4 CoreXL Firewallインスタンスの数と同じになるように設定します。
	e. 選択**Exit**
	f. Security Gatewayを再起動します。
	6. Security Groupでコマンドラインに接続します。
	7. Gaia Clish、またはエキスパートモードにログインします。
	8. IPv6 CoreXL Firewallインスタンスの数を表示します。次を実行します:
	`fw6 ctl multik stat`
	9. IPv4 CoreXL Firewallインスタンスの数を表示します。次を実行します:
	`fw ctl multik stat`
	出力例:

ステップ	手順
	[Expert@GW:0]# fw6 ctl multik stat ID | Active | CPU | Connections | Peak ---------- 0 | Yes | 3 | 0 | 0 1 | Yes | 2 | 0 | 4 2 | Yes | 1 | 0 | 2 [Expert@GW:0]# [Expert@GW:0]# fw ctl multik stat ID | Active | CPU | Connections | Peak ---------- 0 | Yes | 3 | 10 | 14 1 | Yes | 2 | 6 | 15 2 | Yes | 1 | 7 | 15 [Expert@GW:0]#

ステップ2 - NAT46ルールの設定

アクセスコントロールポリシーで、NAT46ルールをManual NATルールとして設定します。

このNATトラフィックを許可するアクセスコントロールルールを追加してください。

1. 該当するソースIPv4オブジェクト(IPv4ホスト、IPv4アドレスレンジ、またはIPv4ネットワーク) を設定します。

   送信元 IPv4 Host オブジェクトを設定するには

   a. **Objects**メニュー > **New Host**をクリックします。

   b. **Object Name**フィールドに、該当する名前を入力します。

   c. **Comment**フィールドに、該当するテキストを入力します。

   d. このオブジェクトの**General**ページをクリックします。

   e. **IPv4 address**フィールドに、IPv4アドレスを入力します。

   f. **IPv6**セクションで:

      何も入力しないでください

   g. このオブジェクトの**NAT**ページで:

      何も設定しないでください。

   h. このオブジェクトの他のページで該当する設定を行います。

   i. クリック**OK**。

送信元 IPv4 ネットワークオブジェクトを設定するには

a. **Objects**メニュー > **New Network**をクリックします。

b. **Object Name**フィールドに、該当する名前を入力します。

c. **Comment**フィールドに、該当するテキストを入力します。

d. このオブジェクトの**General**ページをクリックします。

e. **IPv4**セクションで:

   i. **Network address**フィールドに、送信元IPv4ネットワークのIPv4アドレスを入力します。

   ii. **Net mask**フィールドに、送信元IPv4ネットワークのネットマスクを入力します。

f. **IPv6**セクションで:

   何も入力しないでください。

g. このオブジェクトの**NAT**ページで:

   何も設定しないでください。

h. クリック**OK**。

送信元 IPv4 アドレス範囲オブジェクトを設定するには

a. **Objects**メニュー > **More object types** > **Network Object** > **Address Range** > **New Address Range**をクリックします。

b. **Object Name**フィールドに、該当する名前を入力します。

c. **Comment**フィールドに、該当するテキストを入力します。

d. このオブジェクトの**General**ページをクリックします。

e. **IPv4**セクションで:

   i. **First IP address**フィールドに、IPv4アドレスの範囲の最初のIPv4アドレスを入力します。

   ii. **Last IP address**フィールドに、IPv4アドレスの範囲の最後のIPv4アドレスを入力します。

f. **IPv6**セクションで:

   何も入力しないでください。

g. このオブジェクトの**NAT**ページで:

   何も設定しないでください。

h. クリックOK。

2. 宛先IPv4 Hostオブジェクトを設定します。

このオブジェクトは、IPv4ソースの接続先である宛先IPv4アドレスを表わします。

変換先IPv4 Hostオブジェクトを設定するには

a. Objectsメニュー > New Networkをクリックします。

b. Object Nameフィールドに、該当する名前を入力します。

c. Commentフィールドに、該当するテキストを入力します。

d. このオブジェクトのGeneralページをクリックします。

e. IPv4セクションで:

i. Network addressフィールドに、宛先IPv4ネットワークのIPv4アドレスを入力します。

ii. Net maskフィールドに、宛先IPv4ネットワークのネットマスクを入力します。

f. IPv6セクションで:

何も入力しないでください。

g. このオブジェクトのNATページで:

何も設定しないでください。

h. クリックOK。

3. 96ビットのプレフィックスで定義されたIPv6アドレスを持つ変換元IPv6ネットワークオブジェクトを設定します。

このオブジェクトは、ソースIPv4アドレスの変換先である、変換されたソースIPv6アドレスを表わします。

96ビットプレフィックスで定義されたIPv6アドレスを持つ変換元IPv6ネットワークオブジェクトを設定するには

a. Objectsメニュー > New Networkをクリックします。

b. Object Nameフィールドに、該当する名前を入力します。

c. Commentフィールドに、該当するテキストを入力します。

d. このオブジェクトのGeneralページをクリックします。

e. IPv4セクションで:

何も入力しないでください。

f. **IPv6**セクションで:

i. **Network address**フィールドに、変換されたソースIPv6アドレスを入力します。

ii. **Prefix**フィールドに、**96**を入力します。

g. このオブジェクトの**NAT**ページで:

何も設定しないでください。

h. クリック**OK**。

4. 変換された宛先IPv6 Hostオブジェクトを設定します。

このオブジェクトは、変換されたIPv4ソースが接続される、変換された宛先IPv6アドレスを表わします。

変換先IPv6ホストオブジェクトを設定するには

a. **Objects**メニュー > **New Host**をクリックします。

b. **Object Name**フィールドに、該当する名前を入力します。

c. **Comment**フィールドに、該当するテキストを入力します。

d. このオブジェクトの**General**ページをクリックします。

e. **IPv4**セクションで:

何も入力しないでください。

f. **IPv6**セクションで:

Network addressフィールドに、宛先の静的 IPv6アドレスを入力します。

g. このオブジェクトの**NAT**ページで:

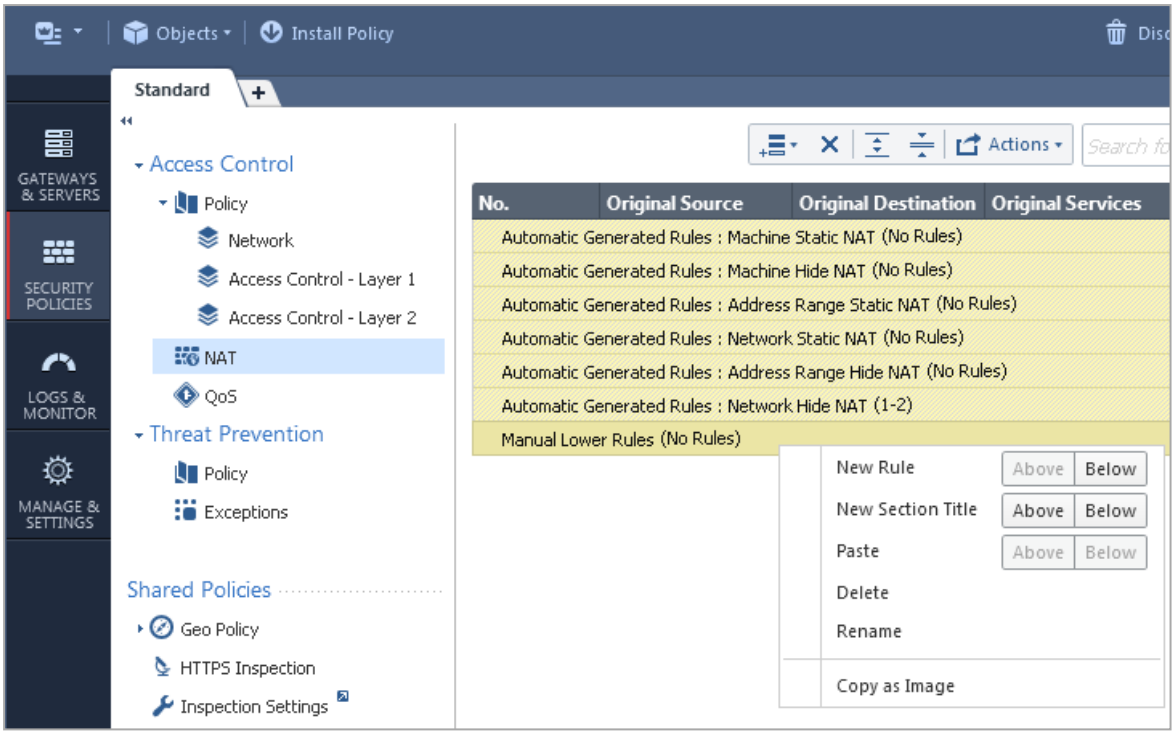
何も設定しないでください。

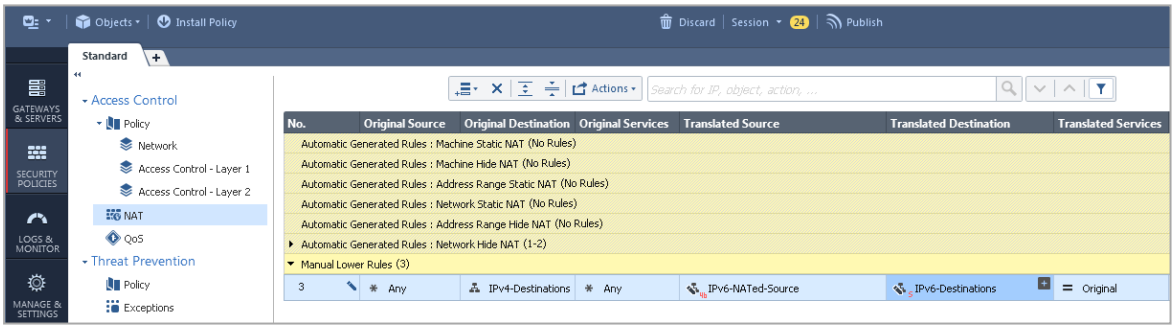
h. このオブジェクトの他のページで該当する設定を行います。

i. クリック**OK**。

5. 手動NAT46ルールを作成します。

手順





a. 左のナビゲーションツールバーから、**Security Policies**をクリックします。

b. 一番上の**Access Control**セクションで、**NAT**をクリックします。

c. **Manual Lower Rules**セクションのタイトルを右クリックし、**New Rule**の近くで、**Above**または**Below**をクリックします。

このNAT46ルールを設定します。

オリジナル発信元	オリジナル宛先	オリジナルサービス	変換発信元	変換宛先	変換サービス
***Any** または 発信元 IPv4 **Host** オブジェクト または 発信元 IPv4 **Address Range** オブジェクト または 発信元 IPv4 **Network** オブジェクト	IPv4 **Host** オブジェクト	***Any**	IPv6 **Network** オブジェクト と IPv6アドレス を持ち、次で 定義： 96ビット プレフィックス	IPv6 **Host** オブジェクト	**= Original**

以下の手順を実行します:

i. **Original Source**カラムに、該当するIPv4オブジェクトを追加します。

このルールカラムでは、NAT46ルールは次のタイプのオブジェクトのみをサポートします。

- `*Any`
- 静的IPv4アドレスを持つホスト
- IPv4アドレスを持つアドレス範囲
- IPv4アドレスを持つネットワーク

ii. **Original Destination**カラムに、IPv4ソースの接続先である宛先IPv4アドレスを表すIPv4**Host**オブジェクトを追加します。

このルールカラムでは、NAT46ルールはIPv4ホストオブジェクトのみをサポートします。

iii. **Original Services**カラムは、デフォルトの**Any**のままにします。

iv. **Translated Source**カラムに、96ビットのプレフィックスで定義されたIPv6アドレスを持つIPv6**Network object**を追加します。

このルールカラムでは、NAT64ルールは、96ビットプレフィックスで定義されたIPv6アドレスを持つIPv6ネットワークオブジェクトのみをサポートします。

v. **Translated Source**カラムで、96ビットのプレフィックスを持つIPv6**Network object**を右クリック > **NAT Method**をクリック > **Stateless NAT46**をクリックします。

46のアイコンが**Translated Source**カラムに表示されます。

vi. **Translated Destination**カラムに、変換されたIPv4ソースが接続する変換された宛先IPv6アドレスを表わすIPv6**Host**オブジェクトを追加します。

このルールカラムでは、NAT46ルールはIPv6ホストオブジェクトのみをサポートします。

vii. **Translated Services**カラムは、デフォルトの**= Original**のままにします。

要約すると、これらのNAT46ルールのみを設定する必要があります(ルール番号は便宜上のものです)。

#	オリジナル 発信元	オリジナル 宛先	オリジナル サービス	変換 発信元	変換 宛先	変換 サービス
1	*Any	IPv4 ホスト オブジェクト	*Any	IPv6 ネットワーク オブジェクト と IPv6アドレス を持ち、次で定義： 96ビット プレフィックス	IPv6 ホスト オブジェクト	= Original
2	IPv4 ホスト オブジェクト with スタティック IPv4 アドレス	IPv4 ホスト オブジェクト	*Any	IPv6 ネットワーク オブジェクト と IPv6アドレス を持ち、次で定義： 96ビット プレフィックス	IPv6 ホスト オブジェクト	= Original

#	オリジナル 発信元	オリジナル 宛先	オリジナル サービス	変換 発信元	変換 宛先	変換 サービス
3	IPv4 *アドレス範囲* オブジェクト	IPv4 *ホスト* オブジェクト	*Any	IPv6 *ネットワーク* オブジェクト と IPv6アドレス を持ち、次で定義： 96ビット プレフィックス	IPv6 *ホスト* オブジェクト	= Original
4	IPv4 *ネットワーク* オブジェクト	IPv4 *ホスト* オブジェクト	*Any	IPv6 *ネットワーク* オブジェクト と IPv6アドレス を持ち、次で定義： 96ビット プレフィックス	IPv6 *ホスト* オブジェクト	= Original

6. アクセスコントロールポリシーをインストールします。

NAT46トラフィックのログ

説明

NAT64接続のSecurity Gatewayログでは、送信元と宛先のIPv6アドレスが元のIPv6形式で表示されます。

NAT46のエントリを確認するには、**Log Details**ウィンドウの**More**セクションをご覧ください。

ログのフィールド	説明
Xlate (NAT) Source IP	Security Gatewayが元のソースIPv4アドレスを変換した、変換後のソースIPv6アドレスを表示します。
Xlate (NAT) Destination IP	Security Gatewayが元の宛先IPv4アドレスを変換した、変換された宛先IPv6アドレスを表示します。
More	エントリをNAT46トラフィックとして識別します(`Nat46 enabled`)

NAT64ルールの操作

メニュー

NAT64 変換 (RFC 6146)は、**IPv6のみのクライアント**が、**ユニキャスト**UDP、TCP、またはICMPを使って**IPv4のみのサーバ**と通信できるようにします。

IPv6専用クライアントでの定義

いずれかの方法を実行します。

- IPv6のみを実装したネットワーキングスタックを持つホスト。
- IPv4とIPv6の両方のプロトコルを実装したネットワークスタックを持つホストで、IPv6のみの接続性を持つもの。
- IPv6専用クライアントアプリケーションを実行するホスト。

IPv4専用サーバの定義

いずれかの方法を実行します。

- IPv4のみを実装したネットワーキングスタックを持つホスト。
- IPv4とIPv6の両方のプロトコルを実装したネットワークスタックを持つホストで、IPv4のみの接続性を持つもの。
- IPv4のみのサーバアプリケーションを実行するホスト。

IPアドレスの変換は、RFC 6145で定義されているIP/ICMP変換アルゴリズムに従ってパケットヘッダを変換することで行われます。IPv4ホストのIPv4アドレスは、RFC 6052で定義されているアルゴリズムを使用してIPv6アドレスに変換され、この特定の目的のためにIPv6プレフィックスがステートフルNAT64に割り当てられます。

注 - DNS64 については、RFC 6147を参照のこと。

ステートフルNAT64のプロパティ

- N:M変換の実行:
  - NはMより大きくなければならない
  - M=1 の場合、単一のIPv4アドレスの背後にHide NATを実行します。
  - M>1 の場合、IPv4 アドレスの範囲の後ろに Hide NAT を実行します。
- IPv4アドレスの保存性が高い(ポートを使って多重化) 。
- 接続状態およびバインディングを保存します。

- IPv6クライアントへのIPv6アドレスの割り当てに関する要件はありません。IPv6アドレスの割り当ては、どのようなモードでも正当です(Manual、DHCP6、SLAAC)。
- スケーラブルなソリューションです。

NAT64の使用例

- [IPv6ネットワーク] --- (インターネット) --- [セキュリティゲートウェイ] --- [内部IPv4ネットワーク]

  コンテンツプロバイダの一般的な使用例。DNS64は必要ありません。

- [内部IPv6ネットワーク] --- [セキュリティゲートウェイ] --- (インターネット) --- [IPv4ネットワーク]

  通信事業者、ISP、企業での一般的な使用例。DNS64が必要です。

- [IPv6ネットワーク] --- [セキュリティゲートウェイ] --- [IPv4ネットワーク]

  企業における一般的な使用例。DNS64が必要です。

NAT64でサポートされている規格

- RFC 6144- IPv4/IPv6変換フレームワーク
- RFC 6146- ステートフルNAT64:IPv6クライアントからIPv4サーバへのネットワークアドレスとプロトコルの変換
- RFC 6052- IPv4/IPv6トランスレータのIPv6アドレス指定
- RFC 6145- IP/ICMP変換アルゴリズム
- RFC 2428- IPv6とNATのためのFTP拡張機能
- RFC 6384- IPv6-IPv4変換のためのFTPアプリケーションレイヤーゲートウェイ(ALG)

NAT64の既知の制限事項

NAT64ルールはサポート**しません**:

- VoIPトラフィック。
- HTTPSインスペクション
- SSLデマルチプレクサ。
- HTTPプロキシモードのセキュリティゲートウェイ。
- IPS保護 "HTTPヘッダスプーフィング"。

NAT64変換フロー例

トポロジ例

[IPv6クライアント] --- (インタフェース) [セキュリティゲートウェイ] (内部) --- [IPv4サーバ]

各変数の意味は以下のとおりです。

項目	説明
IPv6クライアント	IPv6実アドレスは1111:1111::0100/96です。
セキュリティゲートウェイ 外部インタフェース	IPv6アドレスは1111:1111::1/96です。
セキュリティゲートウェイ 内部インタフェース	IPv4アドレスは10.0.0.1/24です。 IPv6アドレスは3333:4444::1/96です。
IPv4サーバ	IPv4実アドレスは10.0.0.100/24です。 IPv6 NATedアドレスは1111:2222::0A00:0064/96です。
IPv6 NATedネットワーク	外部Security Gateway側のネットワークのIPv6アドレスは1111:2222::/96 です。 これらのIPv6アドレスは、IPv4サーバのIPv4アドレスをIPv6アドレスに変換するために使用されます。
IPv4 NATedネットワーク	内部Security Gateway側のネットワークのIPv4アドレスは 1.1.1.0/24です。 これらのIPv4アドレスは、IPv6クライアントのIPv6アドレスをIPv4アドレスに変換するために使用されます。

トラフィックフローの例

1. IPv6クライアントは、IPv4サーバのNATされたIPv6アドレスにIPv6接続を開始します。

   IPv6クライアントのIPv6実アドレス1111:1111::0100からIPv4サーバのNATされたIPv6アドレス1111:2222::0A00:0064まで

   各変数の意味は以下のとおりです。

   「1111:2222::」の部分は、NATされたIPv6サブネットです

   「0A00:0064」の部分が10.0.0.100

2. Security Gatewayは、これらのNAT変換を実行します。

a. IPv6クライアントのソースアドレスを、実際のIPv6アドレス1111:1111::0100から、特別な連結ソースIPv6アドレス0064:FF9B::0101:01Xに変換します。

各変数の意味は以下のとおりです。

「0064:FF9B::」の部分は、NAT64用に予約された周知のプレフィックス(RFCで定義)

「0101:01XX」の部分が1.1.1.X

b. IPv6クライアントのソースアドレスを、特別に連結されたソースIPv6アドレス0064:FF9B::0101:01XXからソースIPv4アドレス1.1.1.Xに変換します。

c. IPv6クライアントのNATed*宛先*アドレスを、IPv6アドレス1111:2222::0A00:0064からNATed宛先IPv4アドレス10.0.0.100に変換します。

3. IPv4サーバは、*送信元IPv4*アドレス1.1.1.Xから*宛先*IPv4アドレス10.0.0.100へのこのリクエスト接続を受信します。

4. IPv4サーバはこの接続に対して、*送信元*IPv4アドレス10.0.0.100から*宛先*IPv4アドレス1.1.1.Xに返信します。

5. Security Gatewayは、これらのNAT変換を実行します。

a. IPv4サーバのソース実IPv4アドレス10.0.0.100を、ソースNATedされたIPv6アドレス1111:2222::0A00:0064に変換します。

b. IPv6クライアントのNATed*宛先*IPv4アドレス1.1.1.Xを、*宛先*特別連結IPv6アドレス0064:FF9B::0101:01Xに変換します。

各変数の意味は以下のとおりです。

「64:FF9B::」の部分は、NAT64用に予約された有名なプレフィックス(RFCで定義)

「0101:01XX」の部分が1.1.1.X

c. IPv6クライアントの*宛先*特別連結IPv6アドレス0064:FF9B::0101:01XXを*宛先*IPv6実アドレス1111:1111::0100に変換します。

6. IPv6クライアントはこのリプライ接続を、*送信元*IPv6アドレス1111:2222::0A00:0064から*宛先*IPv6アドレス1111:1111::0100への接続として受信します。

概要例

- *リクエスト*: [IPv6クライアント] ---> [セキュリティゲートウェイ] ---> [IPv4サーバ]

パケット内のフィールド	元のIPv6パケット	NATed IPv4パケット
ソースIP	1111:1111::0100 / 96	1.1.1.X / 24
宛先IP	1111:2222::0A00:0064 / 96	10.0.0.100 / 24

- *返信*: [IPv6クライアント] <--- [セキュリティゲートウェイ] <--- [IPv4サーバ]

パケット内のフィールド	元のIPv4パケット	NATed IPv6パケット
ソースIP	10.0.0.100 / 24	1111:2222::0A00:0064 / 96
宛先IP	1.1.1.X / 24	1111:1111::0100 / 96

NAT64の設定

ステップ1 - NAT64用セキュリティゲートウェイの準備

注 -クラスタでは、すべてのクラスタメンバを同じ方法で設定する必要があります。

ステップ	手順
1	宛先IPv4ネットワークに接続するインタフェースにIPv6アドレスが割り当てられ、IPv6ネットワークのプレフィックス長が**96**以下であることを確認します。 **注** - これは、IPv6ネットワークプレフィックス長が**96**以下の有効なIPv6アドレスであれば、どれでもかまいません。 ■ Gaia Portal: **Network Management > Network Interfaces**をクリックします。 ■ Gaia Clish: 次を実行します: `show interface <Name of Interface> ipv6-address` IPv6アドレスが割り当てられていない場合は、今すぐ割り当ててください。 詳細 : *R82 Gaia Administration Guide- ネットワーク管理章 - セクション ネットワークインタフェース - セクション 物理インタフェース*

ステップ	手順

2	IPv6ルーティングが、NATされたIPv6アドレス(NAT64ルールの*Original Destination* カラムに定義されている) 宛てのトラフィックを、宛先IPv4ネットワークに接続するインタフェースを介して送信するように設定されていることを確認します。
	■ Gaia Portal:
	Advanced Routing > Routing Monitorをクリックします。
	■ Gaia Clish:
	次を実行します:
	`show ipv6 route`
	もし、そのようなルートがまだ存在しない場合は、Gaia Clishで追加してください。
	詳細 : *R82 Gaia Administration Guide*。
	これらのコマンドをGaiaClishで実行します。
	a. スタティックルートを追加します。
	`set ipv6 static-route <NATed Destination IPv6 Addresses>/<96 or less> nexthop gateway <Any IPv6 Address from the IPv6 subnet of the Interface that connects to the destination real IPv4 network> on`
	トポロジの例:
	[IPv6 Client] --- (NATed IPv6 of IPv4 side are 1111:2222::/96) [Security Gateway] (eth3 with IPv6 3333:4444::1) --- [IPv4 Server]
	この場合、次のコマンドでIPv6ルートを設定します。
	`set ipv6 static-route 1111:2222::/96 nexthop gateway 3333:4444::10 on`
	b. 設定を保存します。
	`save config`

ステップ	手順

3	IPv6 CoreXL Firewallインスタンスの数が、IPv4 CoreXL Firewallインスタンスの数と**同じ**であることを確認します。
	1. Security Groupでコマンドラインに接続します。
	2. Gaia Clish、またはエキスパートモードにログインします。
	3. IPv6 CoreXL Firewallインスタンスの数を表示します。
	`fw6 ctl multik stat`
	4. IPv4 CoreXL Firewallインスタンスの数を表示します。
	`fw ctl multik stat`
	5. IPv6 CoreXL Firewallインスタンスの数がIPv4 CoreXL Firewallインスタンスの数より少ない場合、次の手順を実行します。
	i. 次を実行します:
	`cpconfig`
	ii. 選択**Check Point CoreXL**
	iii. 選択**Change the number of IPv6 firewall instances**
	iv. IPv6 CoreXL Firewallインスタンスの数をIPv4 CoreXL Firewallインスタンスの数と同じになるように設定します。
	v. 選択**Exit**
	vi. Security Gatewayを再起動します。
	6. Security Groupでコマンドラインに接続します。
	7. Gaia Clish、またはエキスパートモードにログインします。
	8. IPv6 CoreXL Firewallインスタンスの数を表示します。
	`fw6 ctl multik stat`
	9. IPv4 CoreXL Firewallインスタンスの数を表示します。
	`fw ctl multik stat`
	出力例:
	`[Expert@GW:0]# fw ctl multik`
	`ID | Active | CPU | Connections | Peak`
	`----------`
	` 0 | Yes | 3 | 10 | 14`
	` 1 | Yes | 2 | 6 | 15`
	` 2 | Yes | 1 | 7 | 15`
	`[Expert@GW:0]#`
	`[Expert@GW:0]# fw6 ctl multik stat`
	`ID | Active | CPU | Connections | Peak`
	`----------`
	` 0 | Yes | 3 | 0 | 0`
	` 1 | Yes | 2 | 0 | 4`
	` 2 | Yes | 1 | 0 | 2`
	`[Expert@GW:0]#`

ステップ2 - NAT64ルールの設定

アクセスコントロールポリシーで、NAT64ルールを手動NATルールとして定義します。

このNATトラフィックを許可するアクセスルールを追加していることを確認してください。

1. ソースIPv6ネットワークオブジェクトを定義します。

   このオブジェクトはソースIPv6アドレスを表わし、ソースIPv4アドレスに変換します。

   手順

   a. **Objects**メニュー > **New Network**をクリックします。

   b. **Object Name**フィールドに、該当する名前を入力します。

   c. **Comment**フィールドに、該当するテキストを入力します。

   d. このオブジェクトの**General**ページをクリックします。

   e. **IPv4**セクションで:

      何も入力しないでください。

   f. **IPv6**セクションで:

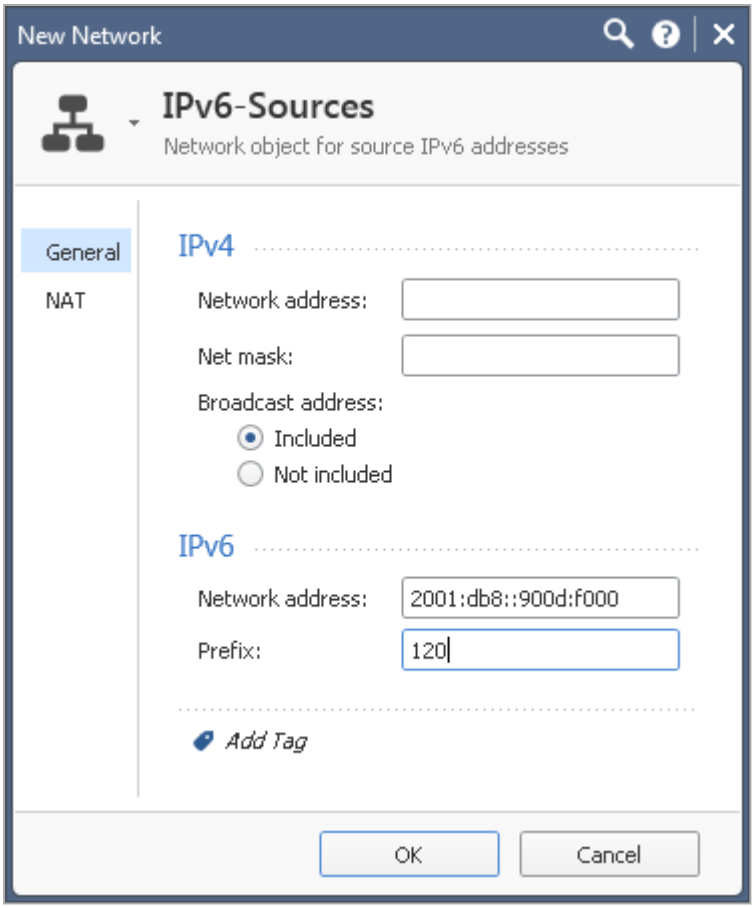
      i. **Network address**フィールドには、ソースIPv4アドレスに変換するIPv6ネットワークのIPv6アドレスを入力します。

      ii. **Prefix**フィールドに、IPv6ネットワークのプレフィックスを入力します。

   g. このオブジェクトの**NAT**ページで:

      何も設定しないでください。

   h. クリック**OK**。



2. IPv4-embedded IPv6アドレスを持つ変換先IPv6ネットワークオブジェクト、または静的IPv6アドレスを持つ変換先IPv6ホストオブジェクトを定義します。

   このオブジェクトは、IPv6ソースが接続する変換された宛先IPv6アドレスを表わします。

   手順

   a. **Objects**メニュー > **New Network**をクリックします。

   b. **Object Name**フィールドに、該当する名前を入力します。

   c. **Comment**フィールドに、該当するテキストを入力します。

   d. このオブジェクトの**General**ページをクリックします。

   e. **IPv4**セクションで：

      何も入力しないでください。

f. **IPv6**セクションで:

i. **Network address**フィールドに、IPv6ソースが接続する宛先*IPv4埋め込み*IPv6アドレス(*IPv4*マッピングIPv6アドレスとも呼ばれる)を入力します。

このようなIPv6アドレスは、左から順に、80個の「0」ビット、16個の「1」ビット、そしてIPv4アドレスの32ビット、0:0:0:0:FFFF:X.Y.Z.W(X.Y.Z.Wは宛先IPv4アドレスの4オクテットを表す)を含んでいます。

例えば、IPv4ネットワーク192.168.3.0の場合、IPv4-embedded IPv6アドレスは0:0:0:0:FFFF:192.168.3.0、または0:0:0:FFFF:C0A8:0300となります。詳細は、RFC 6052を参照してください。

これらのIPv4-embedded IPv6アドレスは、外部のDNS64サーバによって公開されます。

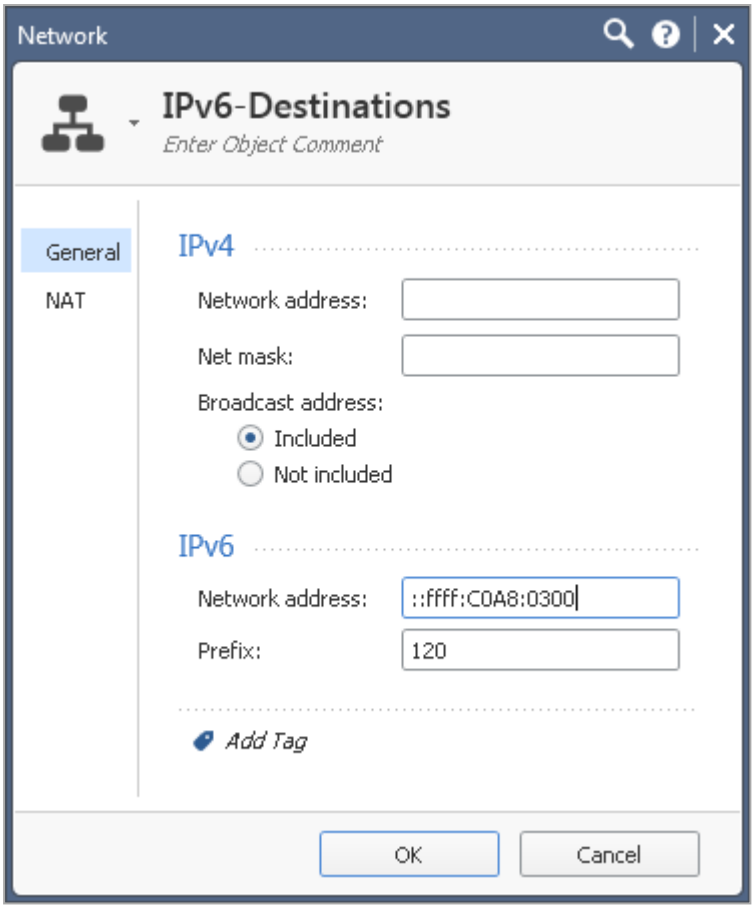
ii. **Prefix**フィールドに、該当するIPv6プレフィックスを入力します。

注 - IPv4埋め込みIPv6アドレスを定義できるのは、アドレス範囲、ネットワーク、ホストのオブジェクトタイプのみです。

g. このオブジェクトの**NAT**ページで:

何も設定しないでください。

h. クリック**OK**。



3. 変換元IPv4 Address Rangeオブジェクトを定義します。

   このオブジェクトは変換されたソースIPv4アドレスを表し、オリジナルのソースIPv6アドレスに変換します。

   手順

   a. **Objects**メニュー > **More object types** > **Network Object** > **Address Range** > **New Address Range**をクリックします。

   b. **Object Name**フィールドに、該当する名前を入力します。

   c. **Comment**フィールドに、該当するテキストを入力します。

   d. このオブジェクトの**General**ページをクリックします。

e. **IPv4**セクションで:

i. **First IP address**フィールドには、ソースIPv6アドレスの変換先となる、IPv4アドレス範囲の最初のIPv4アドレスを入力します。

ii. **Last IP address** フィールドには、ソースIPv6アドレスの変換先となる、IPv4アドレス範囲の最後のIPv4アドレスを入力します。

注:

- このIPv4アドレス範囲は、プライベートIPv4アドレスを使用してはならない(参照 : RFC 1918、**Menu > Global properties >Non Unique IP Address Range**
- このIPv4アドレスの範囲は、ネットワークのIPv4側で使用しないでください。
- より多くのNAT64同時接続を行うために、大きなIPv4アドレス範囲を定義することをお勧めします。

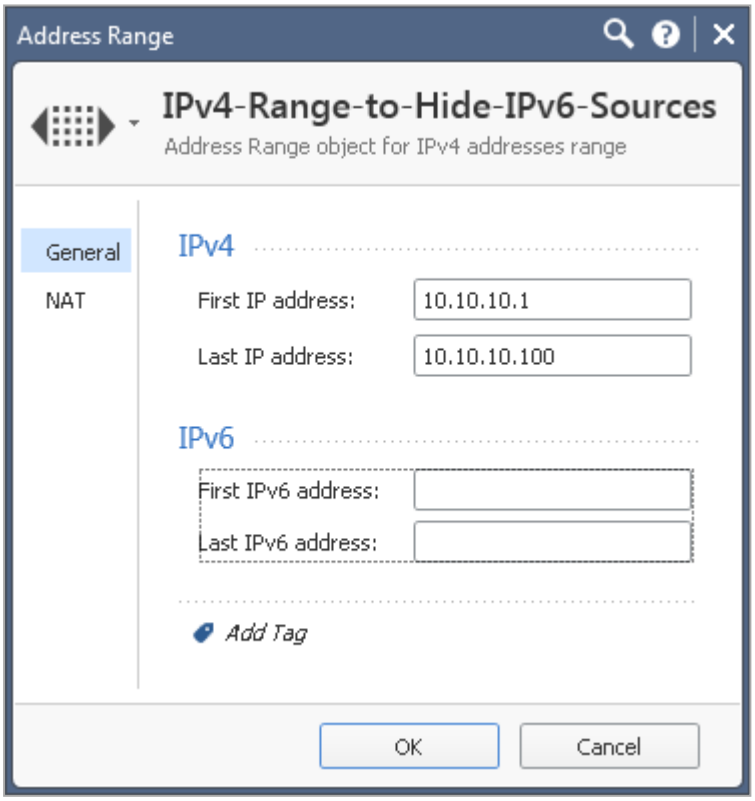
f. **IPv6**セクションで:

何も入力しないでください。

g. このオブジェクトの**NAT**ページで:

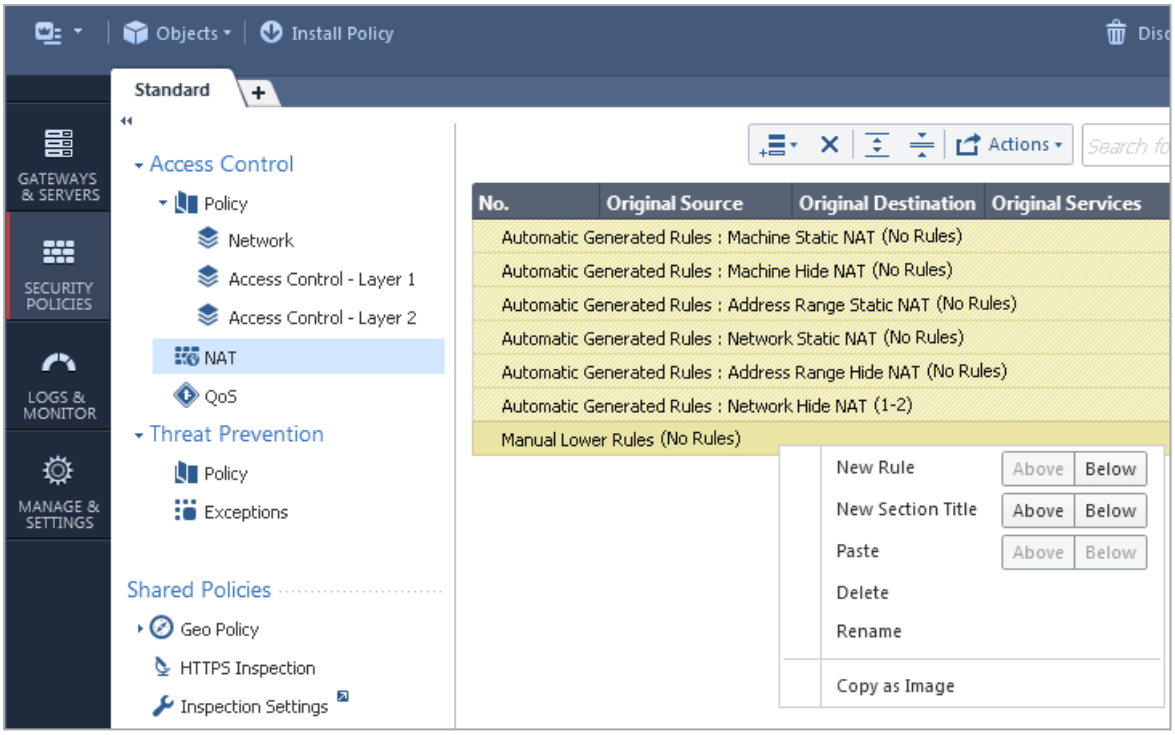
何も設定しないでください。

h. クリック**OK**。



4. 手動NAT64ルールを作成します。

手順



a. 左のナビゲーションツリーから、Security Policiesをクリックします。

b. 一番上のAccess Controlセクションで、NATをクリックします。

c. **Manual Lower Rules**セクションのタイトルを右クリックし、**New Rule**の近くで、**Above**または**Below**をクリックします。

このManual NAT64ルールを設定します。

重要 - いくつかのオブジェクトタイプの組み合わせは、*Original Source*および*Original Destination*カラムではサポートされていません。このセクションの一番下にあるサポートされているNATルールのサマリ表を参照してください。

i. **Original Source**カラムに、元のソースIPv6アドレスのIPv6オブジェクトを追加します。

このルールカラムでは、NAT64ルールは次のタイプのオブジェクトのみをサポートします。

- `*Any`
- 静的IPv6アドレスを持つホスト
- IPv6アドレスを持つアドレス範囲
- IPv6アドレスを持つネットワーク

ii. **Original Destination**カラムに、IPv4-embedded IPv6 アドレスを持つ変換宛先IPv6オブジェクトを追加します。

このルールカラムでは、NAT64ルールは次のタイプのオブジェクトのみをサポートします。

- 静的IPv6アドレスを持つホスト
- IPv4-embedded IPv6アドレスのアドレス範囲
- IPv4-embedded IPv6アドレスのネットワーク

iii. **Original Services**カラムは、デフォルトの**Any**のままにします。

iv. **Translated Source**カラムに、変換ソースIPv4アドレス範囲のIPv4**Address Range** オブジェクトを追加します。

このルールカラムでは、NAT64ルールは次のタイプのオブジェクトのみをサポートします。

- 静的IPv4アドレスを持つホスト、**Original Source**カラムで静的IPv6アドレスを持つホストを選択した場合のみ。
- IPv4アドレスを持つアドレス範囲

v. **Translated Source**カラムで、IPv4**Address Range**オブジェクトを右クリック > **NAT Method**をクリック >**Stateful NAT64**をクリックします:

- **Translated Packet Destination**カラムは、**= Embedded IPv4 Address**を示しています。
- **64**のアイコンは、**Translated Source**と**Translated Destination**のカラムに表示されます。

このルールカラムでは、NAT64ルールはこれらのタイプのオブジェクトのみをサポートしています。

- 静的IPv4アドレスを持つホスト、**Original Source**カラムで静的IPv6アドレスを持つホストを選択した場合のみ。
- Embedded IPv4アドレス

vi. **Translated Services**カラムは、デフォルトの**= Original**のままにします。

d. アクセスコントロールポリシーをインストールします。

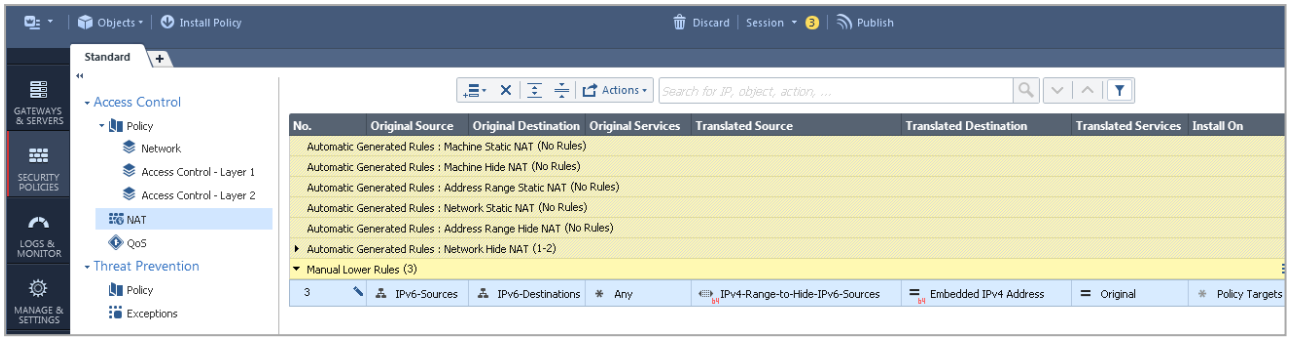
5. アクセスコントロールポリシーをインストールします。

まとめると、以下のManual NAT64ルールのみを設定する必要があります(ルール番号は便宜上つけたものです) 。

#	オリジナル 発信元	オリジナル 宛先	オリジナル サービス	変換 発信元	変換 宛先	変換 サービス
1	*Any	IPv6 *ホスト* オブジェクトと スタティック IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	IPv4 *ホスト* オブジェクト	= Original
2	*Any	IPv6 *アドレス範囲* オブジェクトと IPv4-embedded IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	Embedded IPv4 Address	= Original

#	オリジナル発信元	オリジナル宛先	オリジナルサービス	変換発信元	変換宛先	変換サービス
3	*Any	IPv6 *ネットワーク* IPv4-embedded を持つオブジェクト IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	Embedded IPv4 Address	= Original
4	IPv6 *ホスト* オブジェクト with スタティック IPv6 アドレス	IPv6 *ホスト* オブジェクトと スタティック IPv6アドレス	*Any	IPv4 *ホスト* オブジェクト	IPv4 *ホスト* オブジェクト	= Original
5	IPv6 *ホスト* オブジェクト with スタティック IPv6 アドレス	IPv6 *アドレス範囲* オブジェクトと IPv4-embedded IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	Embedded IPv4 Address	= Original
6	IPv6 *ホスト* オブジェクト with スタティック IPv6 アドレス	IPv6 *ネットワーク* オブジェクトと IPv4-embedded IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	Embedded IPv4 Address	= Original
7	IPv6 *アドレス範囲* オブジェクト	IPv6 *ホスト* オブジェクトと スタティック IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	IPv4 *ホスト* オブジェクト	= Original

#	オリジナル発信元	オリジナル宛先	オリジナルサービス	変換発信元	変換宛先	変換サービス
8	IPv6 *アドレス範囲* オブジェクト	IPv6 *アドレス範囲* オブジェクトと IPv4-embedded IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	Embedded IPv4 Address	= Original
9	IPv6 *アドレス範囲* オブジェクト	IPv6 *ネットワーク* オブジェクトと IPv4-embedded IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	Embedded IPv4 Address	= Original
10	IPv6 *ネットワーク* オブジェクト	IPv6 *ホスト* オブジェクトと スタティック IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	IPv4 *ホスト* オブジェクト	= Original
11	IPv6 *ネットワーク* オブジェクト	IPv6 *アドレス範囲* オブジェクトと IPv4-embedded IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	Embedded IPv4 Address	= Original
12	IPv6 *ネットワーク* オブジェクト	IPv6 *ネットワーク* オブジェクトと IPv4-embedded IPv6アドレス	*Any	IPv4 *アドレス範囲* オブジェクト	Embedded IPv4 Address	= Original



ステップ3 - NAT64の追加設定

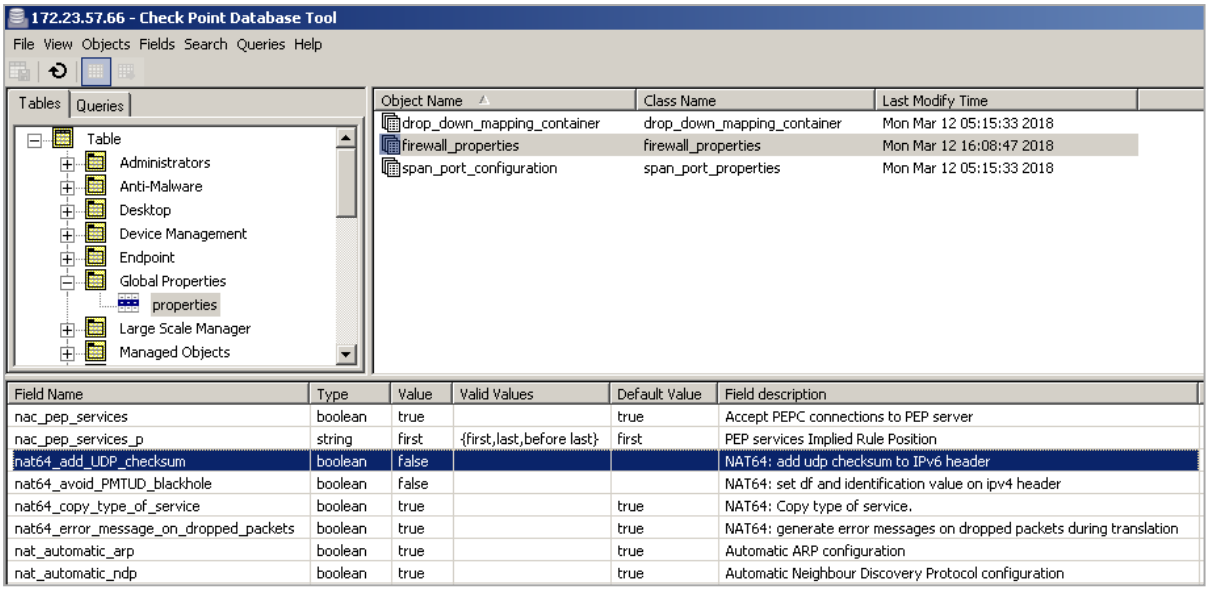
NAT64の変換メカニズムを制御する追加設定を行うことができます。

これらの設定はRFC 6145 に準拠しています。

ベストプラクティス - デフォルト設定の変更は、技術に精通している方のみ行うことをお勧めします。

手順

1. Management Serverに接続しているSmartConsoleのウィンドウをすべて閉じます。
2. 接続 : *Database Tool (GuiDBEdit Tool)*を該当するSecurity Management Serverまたはドメイン管理サーバに送信します。
3. 左上のセクションで、**Table** >**Global Properties** >**properties** をクリックします。
4. 右上のセクションで、**firewall_properties** をクリックします。
5. 下のセクションで、これらの**Field Names**にスクロールしてください。
   - `nat64_add_UDP_checksum`
   - `nat64_avoid_PMTUD_blackhole`
   - `nat64_copy_type_of_service`
   - `nat64_error_message_on_dropped_packets`



6. **Field Name**カラムで該当するパラメータを右クリックし、**Edit**をクリックします。
7. 該当する**Value** (`true`または`false`) を選択し、**OK**をクリックします。

フィールド名	説明
`nat64_add_UDP_checksum`	このパラメータは、パケットのチェックサム値がゼロの場合に、トランスレータが有効なUDPチェックサム値を計算してパケットに追加するかどうかを制御します。 デフォルトでは、チェックサム値がゼロのIPv4 UDPパケットはIPv6側でドロップされるため、これは重要なことです。 **デフォルト:** `false`
`nat64_avoid_PMTUD_blackhole`	このパラメータは、PMTU発見中にIPv4(宛先)側でパケットの断片化を許可するかどうかを制御します。 機器の組み合わせによっては、PMTUの検出に失敗する場合は、この設定を有効にします。 **デフォルト:** `false`
`nat64_copy_type_of_service`	このパラメータは、トラフィック**Class**フィールドを**Type Of Service**フィールドにコピーし、変換されたパケットの**Type Of Service**フィールドをゼロに設定するかどうかを制御します。 **デフォルト:** `true`

フィールド名	説明
`nat64_error_message_on_dropped_packets`	このパラメータは、接続が閉じられた後に監査ログを生成するかどうかを制御します。 閉じた接続ごとに、ログに表示されます。 ■ 接続情報(送信元と宛先のIPアドレス、送信元ポート、サービス)。 ■ 変換されたソースIPアドレスとソースポート。 ■ 開始時刻と終了時刻。 ■ 接続が期限切れで切断された場合、ログには**TCP End Reason**フィールドに追加情報が表示されます。 このフィールドがログに表示されない場合は、接続はTCP RST、またはTCP FINで閉じられ、期限切れではありません。 **デフォルト:** `true`

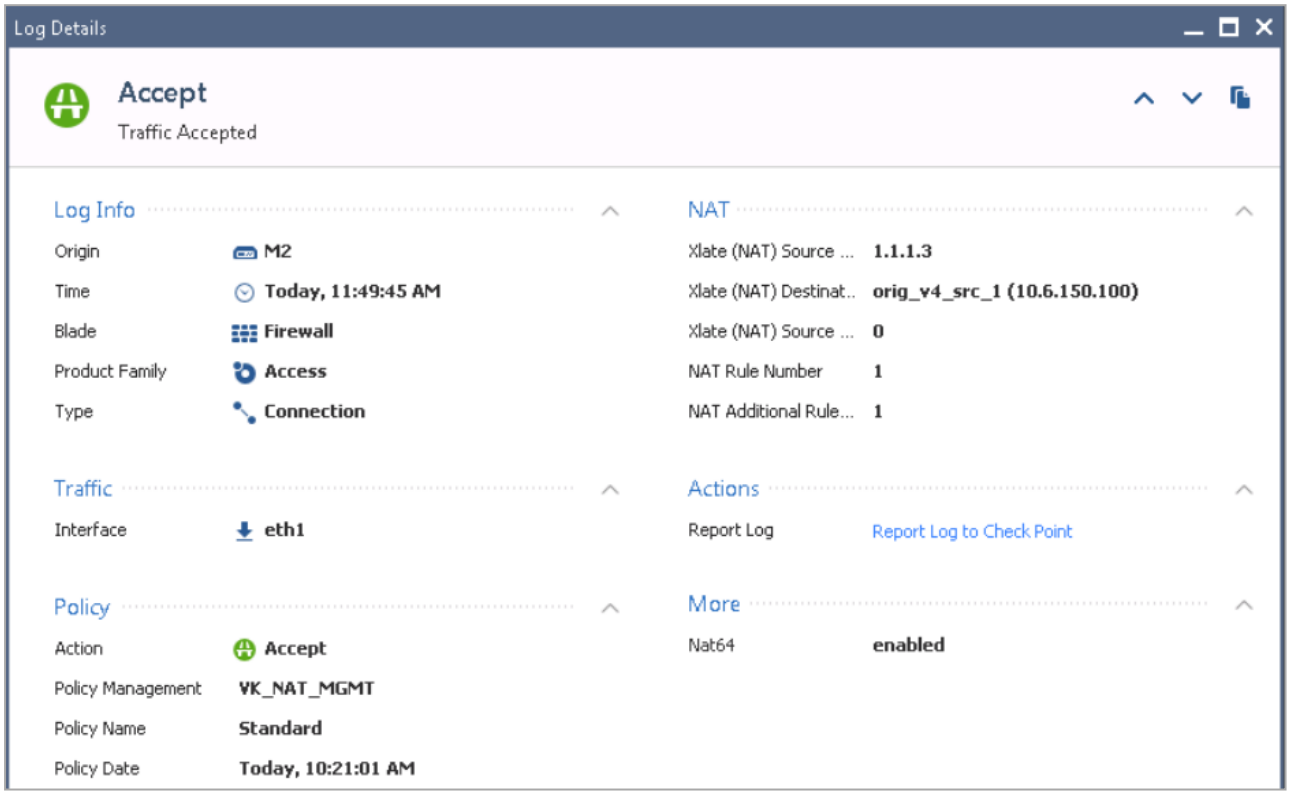
8. 変更を保存します(**File > Save All**をクリック)。
9. データベースツール(GuiDBEditツール)を閉じます。
10. SmartConsoleで該当するSecurity Management ServerまたはDomain Management Serverに接続します。
11. アクセスコントロールポリシーをインストールします。

NAT64トラフィックのログ記録

説明

NAT64接続のSecurity Gatewayログでは、送信元と宛先のIPv6アドレスが元のIPv6形式で表示されます。

NAT64エントリを特定するには、**Log Details**ウィンドウで、**More**セクションを見ます。



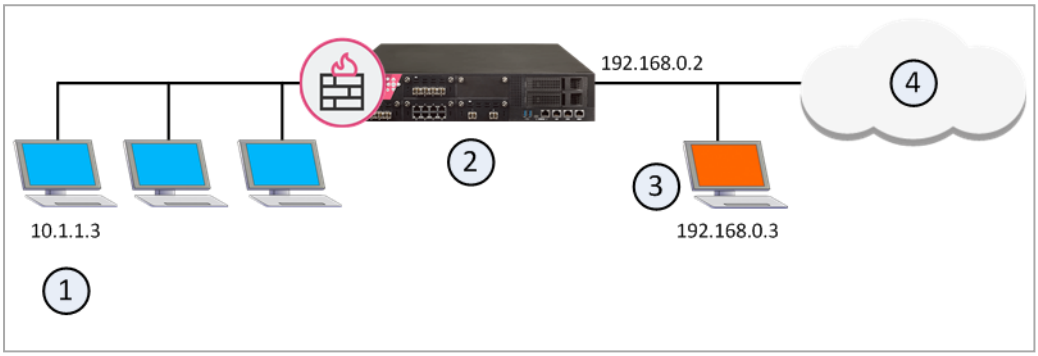
ログのフィールド	説明
Xlate (NAT) Source IP	Security Gatewayが元のソースIPv6アドレスを変換した、変換後のソースIPv4アドレスを表示します。
Xlate (NAT) Destination IP	Security Gatewayが元の宛先IPv6アドレスを変換した変換先IPv4アドレスを表示します。
More	エントリをNAT64トラフィックとして識別します(`Nat64 enabled`)

高度なNAT設定

このセクションでは、特定のシナリオにおける高度なNAT設定について説明します。

自動およびプロキシ ARP

NATを使って内部ネットワーク上のコンピュータに外部ネットワークからのIPアドレスを与えると、そのコンピュータは外部ネットワーク上に表示されるようになります。Security GatewayのNATが自動的に設定されている場合、外部ネットワークから内部コンピュータのIPアドレスに対して送信されるARP Requestに対して、Security Gatewayは変換されたネットワークオブジェクトに代わって返信を行います。



項目	説明
1	内部ネットワーク上のコンピュータ(IPアドレス: 10.1.1.3)
2	外部インタフェースIPアドレス192.168.0.2のセキュリティゲートウェイは、変換された内部オブジェクトに代わってARPリクエストに応答
3	外部ネットワーク上の変換IPアドレス 192.168.0.3
4	外部ネットワーク

手動NATルールを使用している場合、変換されたIPアドレスと同じネットワーク上にあるSecurity GatewayインタフェースのMACアドレスを関連付けるために、プロキシARPエントリを設定する必要があります。

設定の詳細については、sk30197を参照:

- IPv4手動NATのプロキシARP。
- Scalable PlatformのためのプロキシARP。

プロキシARPエントリは、CGNATが変換したアドレス範囲に対しては自動的に生成されません。この問題を解決するには、プロキシARPエントリを手動で設定します。sk30197を参照してください。

IPv6手動NATのプロキシNDPの設定についてはsk91905を参照してください。

NATとアンチスプーフィング

NATは、パケットの送信元IPアドレスに対してのみ行われるアンチスプーフィングチェックの後に実行されます。

つまり、NATと同様にSecurity Gatewayのインタフェースにスプーフィング保護が設定されます。

VPNトンネルのNATを無効にする

VPN内で通信を行う場合、通常はNATを行う必要はありません。

VPNコミュニティオブジェクトを1回クリックするだけで、VPNトンネル内のNATを無効化することができます。

NATルールを定義してVPNトンネルのNATを無効にすると、VPNのパフォーマンスが遅くなります。

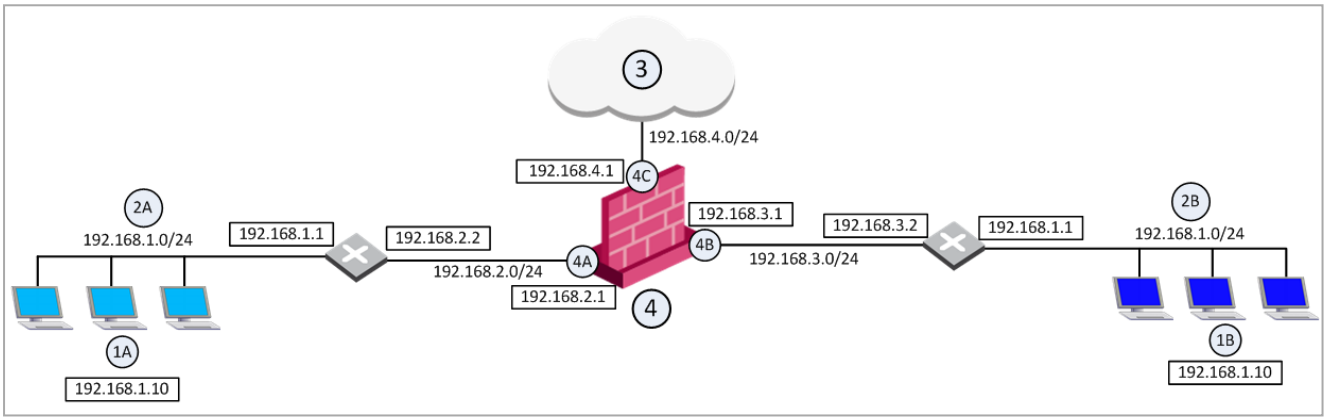
アドレスが重複する社内通信

2つの内部ネットワークでIPアドレスが重複している(または一部重複している)場合、Security Gatewayが有効になります。

- 重複する内部ネットワーク間の通信。
- 重複する社内ネットワークと社外との通信。
- 重複する内部ネットワークごとに異なるセキュリティポリシーの実施。

ネットワーク設定例

トポロジの例:



例えば、ネットワーク2Aとネットワーク2Bが同じアドレス空間(**192.168.1.0/24**)を共有しているとします。

したがって、標準的なNATを使って2つのネットワーク間の通信を可能にすることはできません。

その代わりに、インタフェースごとにオーバーラッピングNATを実行する必要があります。

- ネットワーク2Aのユーザがネットワーク2Bのユーザと通信するには、**192.168.30.0/24**ネットワークを宛先として使用する必要があります。
- ネットワーク2Aのユーザと通信したいネットワーク2Bのユーザは、**192.168.20.0/24**ネットワークを宛先として使用する必要があります。

セキュリティゲートウェイ(4)は、このようにして個々のインタフェースごとにIPアドレスを変換します:

インタフェース	インタフェースでのIPアドレス変換
4A	■ インバウンドのソースIPアドレスは、仮想ネットワーク**192.168.20.0/24**に変換されます。 ■ 送信先のIPアドレスは、**192.168.1.0/24**ネットワークに変換されます。

インタフェース	インタフェースでのIPアドレス変換
4B	■ インバウンドのソースIPアドレスは、ネットワーク192.168.30.0/24に変換されます。 ■ 送信先のIPアドレスは、192.168.1.0/24ネットワークに変換されます。
4C	このインタフェースには重複NATは設定されていません。 代わりに、通常の方法でNAT Hideを使用して(インタフェース単位ではありません) 、インタフェースのIPアドレス(192.168.4.1) の背後にソースアドレスを隠します。

コミュニケーション例

例1 - 内部ネットワーク間の通信

ネットワーク2AのIPアドレス192.168.1.10のユーザ1Aが、ネットワーク2BのIPアドレス192.168.1.10(同じIPアドレス) のユーザ1Bに接続したい場合、ユーザ1AはIPアドレス192.168.30.10への接続を開始します。

を有効にする方法について説明します

ステップ	ソースIPアドレス	宛先IPアドレス
インタフェース4A - NAT前	192.168.1.10	192.168.30.10
インタフェース4A - NAT後	192.168.20.10	192.168.30.10
Security Gatewayは、ネットワーク192.168.20.0/24からネットワーク192.168.30.0/24までのパケットに対してセキュリティポリシーを実施します。		
インタフェース4B - NAT前	192.168.20.10	192.168.30.10
インタフェース4B - NAT後	192.168.20.10	192.168.1.10

例2 - 内部ネットワークとインターネット間の通信

ネットワーク2AのIPアドレス192.168.1.10のユーザー1Aは、インターネット(3)のIPアドレス192.0.2.10に接続します。

社内ネットワークとインターネット間の通信

ステップ	ソースIPアドレス	宛先IPアドレス
インタフェース4A - NAT前	192.168.1.10	192.0.2.10

社内ネットワークとインターネット間の通信 (続き)

ステップ	ソースIPアドレス	宛先IPアドレス
インタフェース4A - NAT後	192.168.20.10	192.0.2.10
セキュリティゲートウェイ(4)は、ネットワーク192.168.20.0/24からインターネット(3)へのパケットに対してセキュリティポリシーを実施します。		
インタフェース4C - NAT前	192.168.20.10	192.0.2.10
インタフェース4C - NAT Hide後	192.168.4.1	192.0.2.10

ルーティングの考慮事項

ネットワーク2Aからネットワーク2B(上の例)へのルーティングを許可するには、セキュリティゲートウェイに必要なルートを設定する必要があります:

宛先ネットワークアドレス	デフォルトゲートウェイ
192.168.20.0 / 24	192.168.2.2
192.168.30.0 / 24	192.168.3.2

設定方法については*R82 Gaia Administration Guide*> "*ネットワーク管理*"の章 > "*IPv4スタティックルート*"セクション。

オブジェクトデータベースの設定

オーバーラップNAT機能を有効にするには*Database Tool (GuiDBEdit Tool)*または、`dbedit`コマンド(sk13301参照)。

この例のネットワークでは、インタフェース4Aとインタフェース4Bのインタフェースごとの値は次のとおりです:

パラメータ	値
enable_overlapping_nat	true
overlap_nat_dst_ipaddr	重複しているIPアドレス(NAT前)。 この例では、両方のインタフェースに192.168.1.0を指定しています。

パラメータ	値
overlap_nat_src_ipaddr	NAT後のIPアドレスです。 この例： ■ インタフェース4Aの192.168.20.0。 ■ インタフェース4Bの192.168.30.0。
オーバーラップネットマスク	重複するIPアドレスのネットマスク。 この例では、255.255.255.0です。

マルチキャスト アクセスコント ロール

マルチキャスト IPは、各 データグラム(IPパケット) のコピーを1つずつマルチキャスト アドレスに送 信し、グループ内 の各 受 信 者 がそのコピーを受 け取 ります。ネット ワーク上 のルータは、マルチキャスト パケットを受 信 するアクセス権 を持 つルータとホストにのみ、データグラムを転 送 します。

マルチキャスト アクセスコント ロールを設 定 するには

1. Security Gatewayオブジェクト を開きます。
2. **Network Management**ページで、インタフェースを選 択 して**Edit**をクリックします。
3. **Interface > Advanced**で、**Drop Multicast packets by the following conditions**をクリックします。
4. インタフェースのマルチキャスト ポリシーを選 択 します。
   - **Drop multicast packets whose destination is in the list**
   - **Drop all multicast packets except those whose destination is in the list**

   IGMPパケット のアウト バウンド でインタフェースのマルチキャスト グループへのアクセスが拒 否 された場 合 、インバウンド パケットも拒 否 されます。

   マルチキャスト パケット のアクセス制 限 を定 義 しない場 合 、セキュリティゲート ウェイのあるインタフェースへのマルチキャスト データグラムは、他 のすべてのインタフェースから出 力 されることが許 可 されます。
5. クリック**Add**。

   Add Objectウィンドウが開き、**Multicast Address Ranges**オブジェクト が選 択 されています。
6. **New >Multicast Address Range** をクリックします。

   Multicast Address Range Propertiesウィンドウが開きます。
7. この範 囲 の名 前 を入 力 します。
8. **IP address Range**または**Single IP Address**を**224.0.0.0 - 239.255.255.255**の範 囲 で定 義 します。

   クラスDのIPアドレスは、マルチキャスト トラフィックのために予 約 され、動 的 に割 り当 てられます。マルチキャスト アドレス範 囲 (`224.0.0.0-239.255.255.255`) は、IPマルチキャスト トラフィックの宛 先 アドレスにのみ使 用 されます。

   宛 先 アドレスが`1110`で始 まるすべてのIPデータグラムは、IPマルチキャスト データグラムです。マルチキャスト アドレス範 囲 の残 りの28ビット は、データグラムの送 信 先 グループを識 別 します。

224.0.0.0-224.0.0.255 の範囲は、ルータによって転送されないLANアプリケーション用に予約されています。これらのアドレスは永続的なホストグループです。例えば、224.0.0.1へのICMPリクエストはネットワーク上のすべてのマルチキャスト対応ホストから応答され、224.0.0.2 はマルチキャスト インタフェースを持つすべてのルータから応答され、224.0.0.13はすべてのPIMルータから応答されます。詳しくは、http://www.iana.org/assignments/multicast-addressesをご覧ください。

マルチキャスト データグラムの送信元アドレスは、常にユニキャストの送信元アドレスとなります。

9. クリックOK。
10. Add Objectウィンドウで、OKをクリックします。
11. Interface Propertiesウィンドウで、OKをクリックします。
12. Security Gatewayウィンドウで、OKをクリックします。
13. ルールベースで、マルチキャスト アドレス範囲をDestinationとして許可するルールを追加します。
14. ルールのServicesに、マルチキャスト プロトコルを追加します。
    - Multicast routing protocols- 例 : PIM(プロトコル独立マルチキャスト) 、DVMRP (距離ベクトルマルチキャスト ルーティングプロトコル) 、MOSPF(OSPFへのマルチキャスト拡張) 。
    - Dynamic registration- ホストは、IGMP(インターネット グループ管理プロトコル) を使用して、指定されたマルチキャスト グループに所属したいことを、最も近いマルチキャスト ルータに知らせます。ホストはいつでもグループを脱退したり、参加したりすることができます。
15. ポリシーをインストールします。

NATの背後にあるSecurity Management

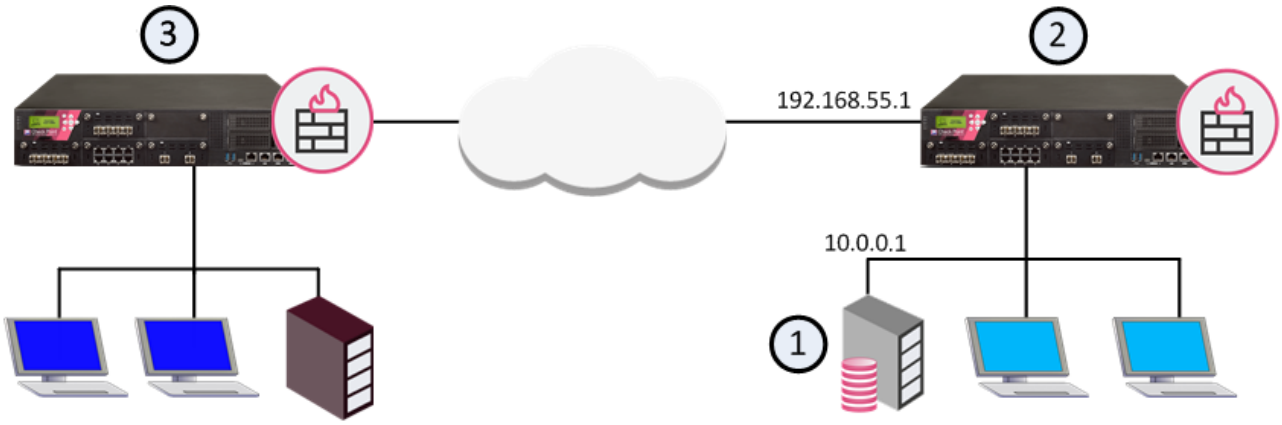
メニュー

説明

Security Management Serverは、パブリックIPアドレスがないため、プライベートIPアドレス(RFC 1918にリストされている) 、または他のルーティング不可能なIPアドレスを使用することがあります。

Security Management Server IPアドレスのNAT(StaticまたはHide) をワンクリックで設定でき、Managed Security Gatewayとの接続を可能にします。Security Management Serverからすべてのセキュリティゲートウェイを制御でき、Security Management Serverへログを送信することができます。また、Management High Availability ServerとLog ServerにもNATを設定することができます。

例:



項目	説明
1	プライマリSecurity Management Server。 ■ 元のIPアドレス - 10.0.0.1 ■ 変換されたIPアドレス - 192.168.55.1
2	Security Management Serverに直接接続されているローカルセキュリティゲートウェイ。 リモートセキュリティゲートウェイは、このローカルセキュリティゲートウェイを介してSecurity Management Serverに接続します。
3	リモートセキュリティゲートウェイは、Security Management Serverに接続する必要があります。

Security Management Serverのコントロール接続用NATの設定

1. 左側のナビゲーションパネルで**Gateways & Servers**をクリックします。
2. Security Management Serverオブジェクトをダブルクリックします。
3. 左側のナビゲーションツリーで、**NAT**をクリックします。
4. **Add Automatic Address Translation rules**を選択します。
5. **Translation method**フィールドで、**Static**を選択します。
6. 該当するIPアドレスを設定します。

   この例の場合 - 192.168.55.1

   注 - ハイアベイラビリティ環境では、各Security Management Serverに1つの静的IPアドレスを設定する必要があります。

7. この2つのオプションから1つを選択します:

   - **Install on Gateway**- このNATを実行するセキュリティゲートウェイ。この例では、Security Management Serverに直接接続されているローカルセキュリティゲートウェイです(図の項目2) 。
   - **Do not create automatic NAT rules**- Security Management Serverは、NATを処理するCheck Point以外のデバイスの背後にあります。

8. **Connections from Security Gateways to this server**。いずれかのオプションを選択します。

   - **Based on topology configuration (use the server's translated or original IP address)**。
   - **Use this server's original IP address**。
   - **Use this server's translated IP address**。

9. オプション: **セキュリティゲートウェイのコントロール接続に適用**を選択 - このオプションは、Security Management Serverとの間のVPNコントロール接続でNATを実行します。これにより、NATゲートウェイを越えてポリシーをインストールしたり、ログを収集したりすることが可能です。
10. クリック**OK**。
11. 該当するセキュリティゲートウェイにアクセスコントロールポリシーをインストールします。

セキュリティゲートウェイの設定

各セキュリティゲートウェイについて、管理サーバ/ログサーバ上の定義を使用するか、管理サーバ/ログサーバの設定を上書きして特定のセキュリティゲートウェイ用に他の設定を行うかを決定できます。

特定のセキュリティゲートウェイに対してNATビハインド管理を設定するには

1. SmartConsoleのゲートウェイとサーバビューで、該当するセキュリティゲートウェイオブジェクトをダブルクリックします。
2. セキュリティゲートウェイObject Editorで、左ナビゲーションメニューから、**NAT** >**Management / Log Servers** を選択します。
3. デフォルトのオプションは**Use Management Server / Log Server settings** です。
4. デフォルト設定を上書きするには、以下のオプションのいずれかを選択します:
   - **Use the remote server's original /translated IP address based on the topology**
   - **Use only the original IP address for the remote servers**。
   - **Use only the translated IP address for the remote servers**。

注

- NATの外側にあるセキュリティ管理サーバは、NATedされたドメインの外から接続を受け取るスタンドアロンサーバ(セキュリティ管理サーバがセキュリティゲートウェイとしても機能する) ではサポートされない(SAMコマンドを受け取るときなど) 。
- このセクションの手順と説明は、NATの背後にあるログサーバにも適用されます。

IPプールNAT

メニュー

IPプールは、セキュリティゲートウェイにルーティング可能なIPアドレスの範囲です。

IPプールNATは、このようなVPN接続シナリオにおいて、暗号化された接続の適切なルーティングを保証します:

- MEP(マルチエントリポイント) セキュリティゲートウェイへのリモートアクセスクライアント
- セキュリティゲートウェイからMEPセキュリティゲートウェイへ

リモートアクセスクライアントまたはセキュリティゲートウェイの背後にあるクライアントから、MEPセキュリティゲートウェイの背後にあるサーバに接続が開かれると、パケットはMEPセキュリティゲートウェイのいずれかを経由してルーティングされます。

接続中のリターンパケットは、接続を維持するために同じセキュリティゲートウェイを経由して戻ってくる必要があります。

これを確実にするために、各MEPセキュリティゲートウェイは、セキュリティゲートウェイにルーティング可能なIPアドレスのプールを維持します。

サーバへの接続が開かれると、Security GatewayはIPプールからIPアドレスを送信元IPアドレスに代入します。

サーバからのリプライパケットはセキュリティゲートウェイに戻り、元の送信元IPアドレスを復元してパケットを送信元に転送します。

NATの優先順位

IPプールNATは、暗号化された接続(VPN)と暗号化されていない接続(Security Gatewayで復号)の両方に使用することができます。

注 - セキュリティゲートウェイを通した**クリア**接続でIPプールNATを有効にするには、該当する**user.def**ファイルで必要なINSPECT設定を行う必要があります(*Management Serverの'user.def'ファイルの場所 (257ページ)*)。必要な場合は*Check Point Support*お問い合わせください。

暗号化されていない接続の場合、IPプールNATはHide NATと比較して以下の利点があります。

- NATされたホストに対して、新しいバック接続(例えばX11)を開くことができます。
- 各IPに1つの接続を許可するプロトコルのユーザとIPサーバのマッピングは、1つのホストだけでなく、複数のホストで動作させることができます。
- IPsec、GRE、IGMPプロトコルは、IPプールNAT(およびスタティックNAT)を使ってNATedできます。Hide NATはTCP、UDP、ICMPプロトコルのみで機能します。

これらの利点から、IPプールNATが同じ接続にマッチする場合、Hide NATよりも優先的に使用するよう指定することができます。Hide NATは、IPプールを使い切った場合のみ適用されます。

NATの優先順位:

1. 静的NAT
2. IPプールNAT
3. Hide NAT

スタティックNATは、IPプールNATの長所とそれ以上の長所をすべて備えているため、他のNAT方式よりも優先順位が高くなります。

インタフェースごとのIPプール

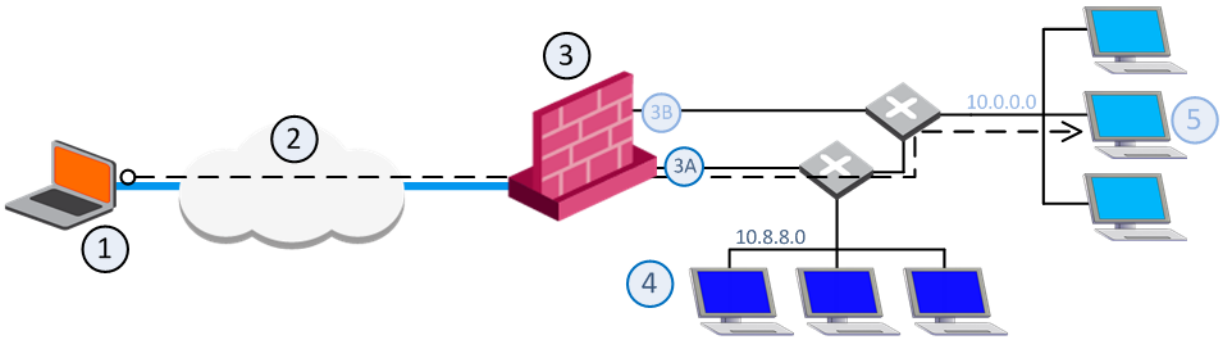
Security Gatewayに単一のIPアドレスプールを定義する代わりに、1つまたは複数のSecurity Gatewayインタフェースに別のIPアドレスプールを定義することができます。

インタフェースごとにIPプールを定義することで、Security Gatewayが2つ以上のインタフェースを持つ場合に発生するルーティングの問題を解決することができます。

リプライパケットを同じSecurity GatewayインタフェースでSecurity Gatewayに戻す必要がある場合があります。

例:

この図の例では、リモートアクセスクライアントからMEPセキュリティゲートウェイへのデプロイメントにおけるMEPセキュリティゲートウェイの1つを示しています:



項目	説明
1	送信元ホストからのパケット: ソース:オリジナル 宛先:
2	インターネット経由のVPNトンネル
3	MEPセキュリティゲートウェイ
3A	IPプール1のパケット: ソース:10.55.8.x 宛先:
3B	IPプール2のパケット: ソース:10.55.10.x 宛先:
4	内部ネットワーク10.8.8.0
5	内部ネットワーク10.10.10.0内の対象ホスト

リモート クライアント が内 部 ネット ワークへの接 続 を開いた場 合 、内 部 ネット ワーク内 のホスト からのリプライパケット は、静 的 IPプールNATアドレスの使 用 により、正 しいSecurity Gatewayインタフェースにルーティングされます。

リモート クライアント のIPアドレスは、Security Gatewayインタフェースの1つのIPプールのアドレスにNATされます。IPプール内 のアドレスは、そのセキュリティゲート ウェイインタフェースを経 由 してのみルーティングできるため、ターゲット ホスト からのすべてのリプライパケット はそのインタフェースにのみ返されます。したがって、インタフェースのIP NATプールが**重 ならない**ようにすることが重 要 です。

パケット がSecurity Gatewayインタフェースに戻 ると、Security Gatewayはリモートピアの送 信 元 IPアドレスを復 元 します。

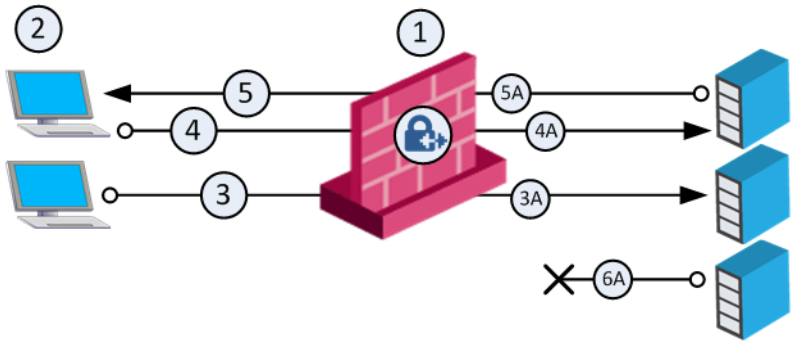
Security Gatewayの背 後 にあるルータのルーティングテーブルを編 集 し、Security GatewayのIPプールからのアドレスが正 しいSecurity Gatewayインタフェースに返 されるようにする必 要 があります。

セキュリティゲート ウェイごとのIPプールNATとインタフェースごとのIPプールNATを切 り替 えてからセキュリティポリシーをインスト ールすると、すべてのIPプールの割 り当 てとNATされた接 続 が削 除 されます。

IPプールアドレスを異 なる宛 先 に再 利 用 する

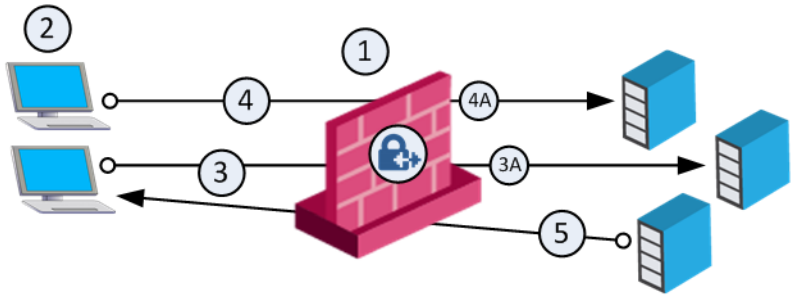
IPプールのアドレスは、異 なる宛 先 に再 利 用 することができ、プール内 のアドレスをより効 率 的 に使 用 することができます。プールにN個 のアドレスが含 まれている場 合 、1つのサーバにN個 以 下 のクライアント が存 在 する限 り、任 意 の数 のクライアント にプールからのIPを割 り当 てることができます。

宛 先 ごとのIPプール割 り当 てを使 用 すると、2つの異 なるクライアント が異 なるサーバと通 信 する限 り、プールから同 じIPを受 け取 ることができます(接 続 1および2) 。IPプールからアドレスを再 利 用 する場 合 、元 のサーバからのバック接 続 のみサポート されます(接 続 3) 。つまり、クライアント へのバック接 続 は、コネクションを開 いた特 定 のサーバからのみ開 くことができます。



項目	説明
1	IPプールアドレスA ~ Zを持つセキュリティゲートウェイ
2	クライアント ソース:オリジナル 宛先:
3A	接続3からのNATされたパケット。 ソース:A 宛先:
4A	接続4からのNATされたパケット。 ソース:A 宛先:
5A	リプライ接続からのNATされたパケット5。 ソース:オリジナル 宛先:A
6A	このサーバはクライアントに戻って宛先Aとの接続を開くことができません。

デフォルトのDo not reuse IP Pool NAT (IPプールNATを再使用しない) 動作は、IPプール内の各IPアドレスが1回ずつ使用されることを意味します(下図の接続1および2)。このモードでは、IPプールに20個のアドレスが含まれる場合、最大20個の異なるクライアントをNATし、任意のソースからクライアントへのバック接続を開くことができます(接続3)。



項目	説明
1	IPプールアドレスA ~ Zを持つセキュリティゲートウェイ。
2	クライアント ソース:オリジナル 宛先:
3A	接続3からのNATされたパケット。 ソース:A 宛先:
4A	接続4からのNATされたパケット。 ソース:Z 宛先:
5	接続。 ソース:オリジナル 宛先:A

再利用モードと**再利用**しないモードを切り替えてからセキュリティポリシーをインストールすると、すべてのIPプール割り当てとすべてのNATされた接続が削除されます。

IPプール設定手順

1. **グローバルプロパティでIPプールNATを有効にする**

    a. SmartConsole **Menu**から、**Global properties**をクリックします。

    b. **グローバルプロパティ>NAT**ページで、**Enable IP Pool NAT**と必要なトラッキングオプションを選択します。

    c. クリック**OK**。

2. **各セキュリティゲートウェイまたはセキュリティゲートウェイインタフェースについて、そのIPプールNATアドレスを表すオブジェクトを作成します。**

   このオブジェクトには、ネットワーク、ネットワークグループ、またはアドレス範囲を指定できます。

   重要:
   - クラスタでは、各クラスタメンバに個別のIPプールを設定する必要があります。
   - 各クラスタメンバインタフェースに個別のIPプールを設定することは**できません**。

   例えば、アドレスレンジの場合、次を実行します:

   a. **Objects Bar (F11)**から、ネットワークオブジェクトツリーで**New > More > Network Object > Address Range > Address Range**を選択します。

   b. **General**タブで、範囲の最初と最後のIPアドレスを入力します。

   c. クリック**OK**。

3. **セキュリティゲートウェイオブジェクトでIPプールNATを有効にして設定します。**

   a. 左側のナビゲーションパネルで**Gateways & Servers**をクリックします。

   b. セキュリティゲートウェイ / クラスタオブジェクトをダブルクリックします。

   c. 左から**NAT**を展開し、**IPプールNAT**をクリックします。

   d. **IPプールNAT**ページで、以下のオプションのいずれかを選択します:

      セキュリティゲートウェイオブジェクトで:

      - **Allocate IP Addresses from**を選択し、作成したアドレス範囲を選択して、セキュリティゲートウェイ全体のIPプールNATを設定します。
      - **Define IP Pool NAT on Gateway interfaces**インタフェースごとにIPプールNATを設定します。

      クラスタオブジェクトで:

      - **Define IP Pool NAT on each cluster member**
      - **Define IP Pool NAT on cluster member interfaces**インタフェースごとにIPプールNATを設定します。

e. **オプション:** これらのオプションを1つ以上選択してください:

- **VPNクライアント接続にIPプールNATを使用する**
- **ゲートウェイ間接続にIPプールNATを使用する**
- **Prefer IP Pool NAT over Hide NAT**を選択し、IPプールNATとHide NATの両方が同じ接続に一致する場合に、IPプールNATを優先するように指定します。Hide NATは、IPプールを使い切った場合にのみ適用されます。

f. **オプション:** 該当する詳細設定を行います。

詳細をクリックし、設定します:

i. **未使用アドレスをIPプールに戻す**

プール内のアドレスは、ユーザがログオフしても60分間(デフォルト)予約されます。ユーザがISPから切断し、リダイヤルして再接続した場合、IPプールからの最初のアドレスがタイムアウトするまで、ユーザには2つのプールNATアドレスが使用されます。ユーザが定期的にISP接続を失う場合、IPプールが枯渇するのを防ぐために、タイムアウトを短くすることができます。

ii. **異なる宛先のためにプールからIPアドレスを再利用する**

クライアントが最初に接続を開いた特定のサーバからだけでなく、あらゆるソースからクライアントへのバック接続を開くことを許可する必要がある場合を除き、これは良いオプションです。

g. クリック**OK**をクリックして**Advanced IP Pool NAT Configuration**ウィンドウを閉じます。

h. クラスタオブジェクトで:

i. 左から**Cluster Members**をクリックします。

ii. 各クラスタメンバをダブルクリックします。

iii. 上部から、**IPプールNAT**タブをクリックします。

iv. **Use IP Pool NAT**を選択します。

v. **Allocate IP addresses from**フィールドで、このクラスタメンバに該当するオブジェクトを選択します。

重要 - クラスタでは、各クラスタメンバに個別のIPプールを設定する必要があります。各クラスタメンバインタフェースに個別のIPプールを設定することは**できません**。

vi. クリック**OK**をクリックしてクラスタメンバプロパティウィンドウを閉じます。

i. クリック**OK**をクリックしてセキュリティゲートウェイ / クラスタオブジェクトを閉じます。

4. **セキュリティポリシーをインストールする**

a. SmartConsoleでSecurity Management Serverに接続します。

b. リモートのセキュリティゲートウェイ/クラスタにアクセスコントロールポリシーをインストールします。

5. **各内部ルータのルーティングテーブルを編集する**

NATプールから割り当てられたIPアドレスを持つパケットが適切なセキュリティゲートウェイ、またはインタフェースごとにIPプールを使用している場合は適切なセキュリティゲートウェイインタフェースにルーティングされるように、該当するルートを設定します。

ネットワークへのモバイル・アクセス

Check Pointのモバイルアクセスを使用することで、リモートユーザがインターネットを利用して簡単かつ安全に社内ネットワークに接続できます。リモートユーザは、Mobile Access Security Gatewayに対して標準的なHTTPSリクエストを開始し、1つまたは複数の安全な認証方式で認証を行います。

モバイルアクセスポータルは、モバイルワーカーやリモートワーカーがインターネット経由で重要なリソースに簡単かつ安全に接続することを可能にします。Check Pointのモバイルアプリは、管理されていないスマートフォンやタブレットから企業のリソースへの安全な暗号化通信を可能にします。アクセスには、社内アプリ、メール、カレンダー、連絡先などがあります。

モバイルアクセスアプリケーションへのアクセスをルールベースに含めるには、**Services & Applications**カラムに**Mobile Application**を含めます。

指定したリモートアクセスクライアントを介してリソースにアクセスできるようにするには、クライアント用のアクセスロールを作成し、ルールの**Source**カラムに含めます。

Check Pointのモバイルアクセスソリューション

Check Point Mobile Accessには、ユーザが遠隔地から社内のリソースにアクセスするための幅広い柔軟なクライアントと機能が備えられています。これらのすべてのソリューションには次の機能が含まれています。

- 企業リソースへのエンタープライズグレードの安全な接続
- 強力なユーザ認証
- きめ細かなアクセスコントロール

モバイルアクセスソリューションとクライアントの最新バージョンの詳細については、sk67820を確認してください。

クライアントベースとクライアントレス

Check Pointのリモートアクセスソリューションは、IPsecおよびSSL暗号化プロトコルを使用して、安全な接続を実現します。空港やホテルなど複雑なトポロジを持つ環境でも、すべてのCheck Pointクライアントが NATデバイス、ホットスポット、およびプロキシを経由して動作することが可能です。リモートアクセスソリューションのインストールの種類は次のとおりです。

- **Client-based**- エンドポイントコンピュータやデバイスにインストールされるクライアントアプリケーション。クライアントは、ユーザのアクセス権限に応じて、ほとんどの種類の企業リソースへのアクセスを提供します。
- **Clientless**- ユーザはWebブラウザで接続し、HTTPS接続を使用します。クライアントレスソリューションは通常、Webベースの企業リソースへのアクセスを提供します。

- **On demand client**- ユーザはWebブラウザで接続し、必要に応じてクライアントがインストールされます。クライアントは、ユーザのアクセス権限に応じて、ほとんどの種類の企業リソースへのアクセスを提供します。

モバイルアクセスクライアント

- Capsule Workspace - モバイルデバイス上に安全なコンテナを作成し、社内Webサイト、ファイル共有、Exchangeサーバへのアクセスをユーザに提供するアプリです。
- Capsule Connect - ユーザにすべてのモバイルアプリケーションへのネットワークアクセスを提供する完全なL3トンネルアプリです。
- Check Point Mobile for Windows - 安全なIPsec VPN接続と認証を提供するWindows IPsec VPNクライアントです。

モバイルアクセスWebポータル

Mobile Access Portalは、Webベースのリソースに安全なアクセスを提供するクライアントレスSSL VPNソリューションです。ユーザはポータルに認証された後、Outlook Web Appや企業Wikiなどの Mobile Accessアプリケーションにアクセスすることができます。

SSL Network Extender

SSL Network Extenderは、オンデマンド型のSSL VPNクライアントであり、インターネットブラウザからコンピュータやモバイル端末にインストールします。内部ネットワークリソースへの安全なアクセスを提供します。

ネットワークリソースへのモバイルアクセスの設定

モバイルアクセスワークフローの例

これは、モバイルアクセスのアプリケーションとリソースへのリモートアクセスを設定するための高レベルのワークフローです。

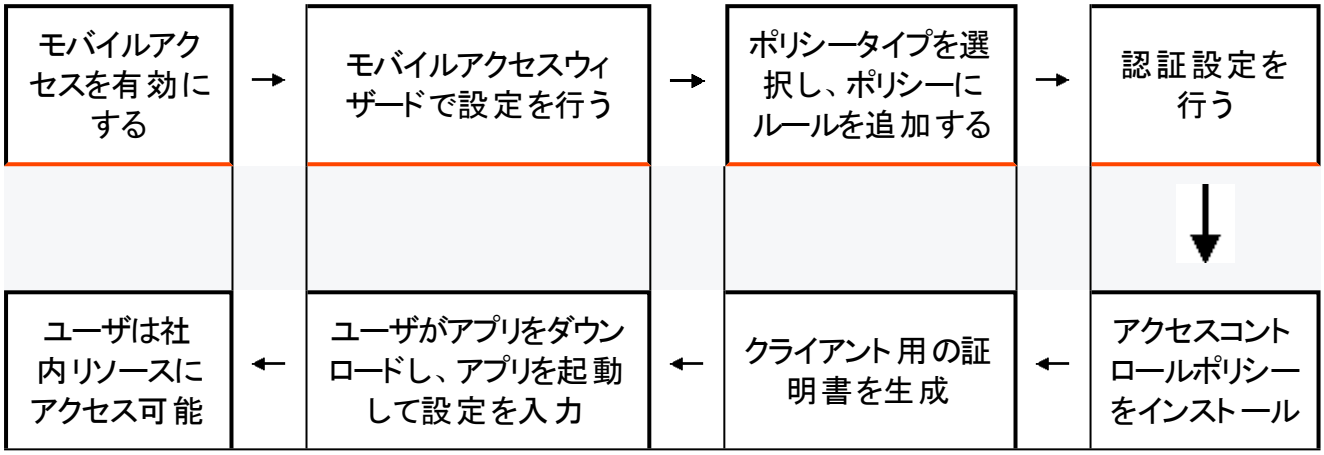
1. SmartConsoleを使用して、セキュリティゲートウェイのMobile Access Software Bladeを有効にします。
2. Mobile Access Configurationウィザードの手順に従って、次の設定を行います。
   a. モバイルクライアントを選択します。
   b. モバイルアクセスポータルを定義します。
   c. Outlook Web Appなどのアプリケーションを定義します。
   d. ADサーバに接続してユーザ情報を取得します。
3. ポリシーの種類を選択します。
   - デフォルトでは、SmartConsoleの**Mobile Access**タブで設定されたレガシーポリシーが使用されます。
   - モバイルアクセスを**Unified Access Control Policy**に含めるには、**Gateway Properties** > **Mobile Access**でこれを選択します。
4. ポリシーにルールを追加します。
   - レガシーポリシーの場合SmartConsoleでルールを追加します。**Security Policies** >**Shared Policies**>**Mobile Access** > を選択します。**Open Mobile Access Policy in SmartConsole**
   - 統合アクセスコントロールポリシー: SmartConsole > **Security Policies Access Control Policy**でルールを追加します。
5. **Gateway Properties** > **Mobile Access** > **Authentication**で認証設定を行います。
6. このSecurity Gatewayオブジェクトにアクセスコントロールポリシーをインストールします。

   ユーザは、設定されたモバイルアクセスポータルを介して、定義された認証方法でモバイルアプリケーションにアクセスできます。
7. オプション: 証明書認証により、Capsule Workspaceアプリを介してユーザに安全なアクセスを提供します。
   a. セキュリティゲートウェイオブジェクト > **Mobile Access** > **Authentication**で、**Settings**をクリックし**Require client certificate**を選択します。

b. 証明書の作成と配布ウィザードを使用します(**Security Policies** > **Client Certificates** > **New**) 。

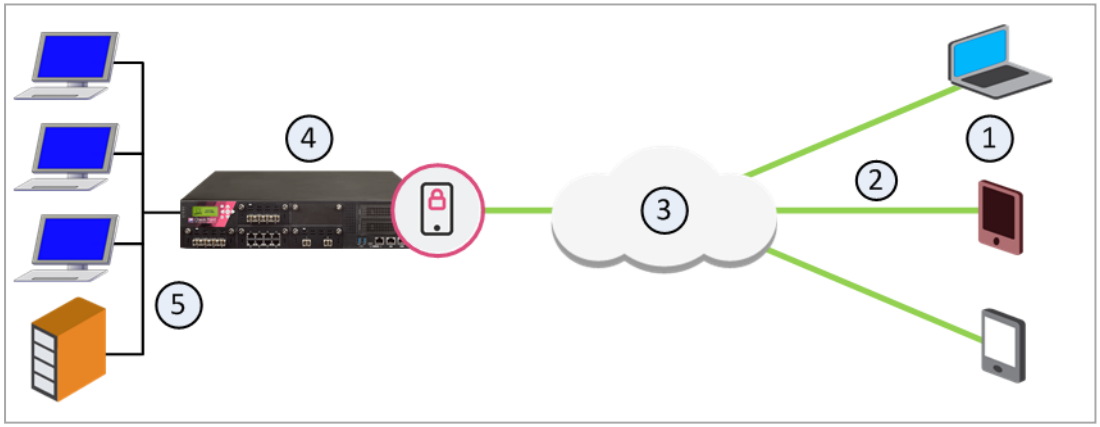
c. ユーザは、Capsule Workspaceアプリをダウンロードします。

d. Capsule Workspaceアプリを開き、Mobile Access Site Nameと必要な認証(ユーザ名やパスワードなど) を入力します。



モバイルアクセスの展開例

これは、内部ネットワークにADとExchangeサーバを持つMobile Access Security Gatewayの導入例です。



項目	説明
1	モバイルデバイス
2	モバイルアクセストンネル
3	インターネット(外部ネットワーク)
4	モバイルアクセスセキュリティゲートウェイ
5	内部ネットワークリソース、AD、Exchangeサーバ

このMobile Accessの導入例では、モバイルデバイスがMobile Accessトンネルを使用して内部ネットワークに接続します。モバイルアクセスセキュリティゲートウェイは、パケットを復号し、ユーザを認証します。接続が許可され、モバイルデバイスが内部ネットワークリソースに接続します。

モバイルアクセス設定ウィザードの使用

この手順では、設定ウィザードを使用してセキュリティゲートウェイ上のMobile Access Software Bladeを有効化し、設定する方法について説明します。このサンプル構成では、ADのユーザグループMobile Accessに、内部ネットワークへの接続を許可されたすべてのユーザが含まれています。この展開は、サンプルモバイルアクセス展開(Sample Mobile Access Deployment) に基づいています。

この構成により、次のクライアントは内部リソースに接続することができます。

- AndroidおよびiOSモバイルデバイス
- WindowsおよびMacコンピュータ
- インターネットブラウザで、内部ネットワークへのSSL Network Extender接続が可能

Mobile Accessを設定するには

1. SmartConsoleで**Gateways & Servers**にアクセスし、Security Gatewayオブジェクトをダブルクリックします。

   General Propertiesウィンドウが開きます。

2. **General Properties** > **Network Security**セクションで、**Mobile Access**を選択します。

   Mobile Access Configuration Wizardの**Mobile Access**ページが開きます。

3. インターネットやモバイルデバイスからの接続を許可するよう、セキュリティゲートウェイを設定します。次のオプションを選択します。

   - **Web**
   - **Mobile Devices**- 必要なオプションを選択します。
   - **Desktops/Laptops**- 必要なオプションを選択します。

4. **Next**をクリックします。

   Web Portalページが開きます。

5. モバイルアクセスポータルのプライマリURLを入力します。

   デフォルトは`https://<IPv4 Address of Security Gateway>/sslvpn`

6. **Next**をクリックします。

   Applicationsページが開きます。

7. 表示するアプリケーションを設定します。

a. **Web Applications**で、**Demo web application (World Clock)**が選択されていることを確認します。

b. **Mail/Calendar/Contacts**で、Exchangeサーバのドメインを入力し、選択します。

- **Mobile Mail (including push mail notifications)**
- **ActiveSync Applications**
- **Outlook Web App**

Mobile Access Portalには、Demo WebとOutlook Web Appのアプリケーションへのリンクが表示されます。モバイルデバイスのクライアントには、他のアプリケーションへのリンクが表示されます。

8. **Next**をクリックします。

Active Directoryページが開きます。

9. ADドメインを選択し、ユーザ名とパスワードを入力します。
10. **Connect**をクリックします。

セキュリティゲートウェイは、ADサーバに接続できることを確認します。

11. **Next**をクリックします。

Usersページが開きます。

Addをクリックし、グループ**Mobile Access**を選択します。

12. **Next**をクリックし、**Finish**をクリックします。.

Mobile Access Configuration Wizardが閉じます。

13. クリック**OK**。

Gateway Propertiesウィンドウが閉じます。

モバイル接続の許可

Mobile Access Configurationウィザードでは、Mobile Access Software Bladeの有効化と設定を行います。コンピュータやデバイスのVPNクライアントからの接続を許可するには、ファイアウォールルールを追加する必要があります。Exchangeサーバ用のホストノードオブジェクトを作成します。他のオブジェクトはすべて事前に定義されています。

名前	発信元	宛先	VPN	サービス	アクション	インストール先	追跡
モバイルアクセスユーザ	Any	ExchngSrvr	RemoteAccess	HTTP HTTPS MSExchange	承認	モバイルアクセスGW	ログ記録

RemoteAccessVPNコミュニティからExchangeサーバへのすべての接続が許可されます。許可されるプロトコルは、HTTP、HTTPS、MS Exchangeのみです。このルールは、Security GatewayのMobileAccessGWグループにインストールされます。

アプリケーションへのアクセスの定義

SmartConsoleのSecurity Policiesページで、ユーザがMobile Accessアプリケーションにアクセスするためのルールを定義します。設定ウィザードで選択されたアプリケーションは、このページに自動的に追加されます。また、これらのSmartConsoleオブジェクトを含むルールを作成、編集することができます。

- ユーザとユーザグループ
- モバイルアクセスアプリケーション
- モバイルアクセスセキュリティゲートウェイ

シングルサインオンの有効化

SSO(シングルサインオン)機能を有効にすると、Mobile Accessセッション中に使用するアプリケーションに対して1度だけ認証を行うことができます。ユーザがMobile Access Portalにログインするために入力する認証情報は、異なるモバイルアクセスアプリケーションの認証に自動的に再利用することができます。SSOのユーザ認証情報は、そのセッションのためにモバイルアクセスセキュリティゲートウェイに安全に保存され、ユーザが異なるリモートデバイスからログインした場合にも再び使用されます。セッションが完了すると、認証情報はデータベースファイルに保存されます。

デフォルトでは、HTTPを使用する新しいMobile Accessアプリケーションで SSOが有効になっています。ほとんどのWebアプリケーションは、指定されたWebフォームでユーザを認証します。Mobile Access Portalからの認証情報を使用するように、アプリケーションのSSOを設定できます。ユーザがアプリケーションごとに再ログインする必要はありません。

SSOを設定するには

1. SmartConsoleで、**Security Policies > Shared Policies > Mobile Access**にアクセスします。
2. **Open Mobile Access Policy in SmartDashboard**をクリックします。
3. **Mobile Access**タブで、**Additional Settings > Single Sign-On**を選択します。

Single Sign-Onページが開きます。

4. アプリケーションを選択してEditをクリックします。

   アプリケーションプロパティウィンドウが開き、Single Sign Onページが表示されます。

Webフォームアプリケーションの場合

1. Application Single Sign-On Method セクションで、Advanced を選択し、Edit をクリックします。

   Advancedウィンドウが開きます。

2. This application reuses the portal credentials. Users are not promptedを選択します。
3. クリックOK。
4. This application uses a Web form to accept credentials from usersを選択します。
5. クリックOK。
6. ポリシーをインストールします。

Citrixサーバへの接続

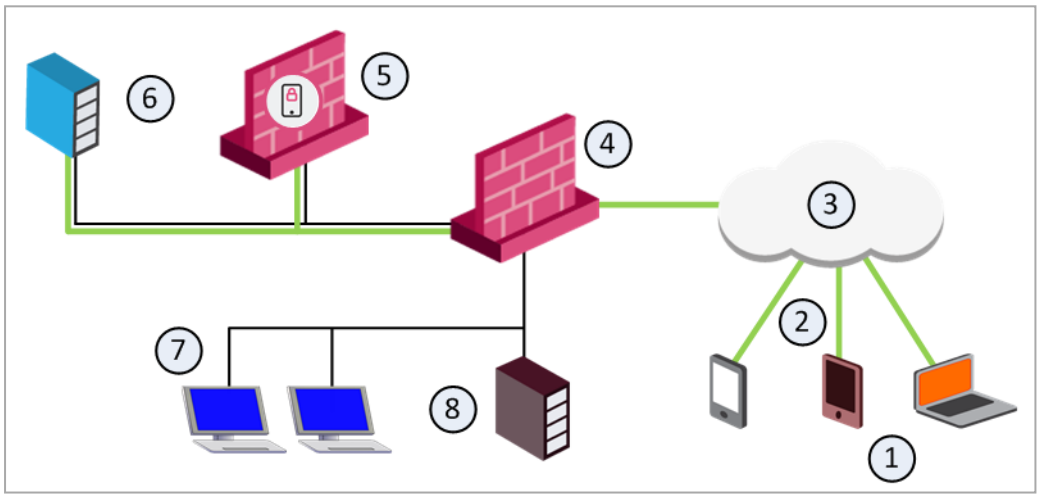
Citrix Services

Mobile Access Software Bladeは、Citrixのクライアントとサービスを統合します。Mobile Accessは独自のSTAエンジンを使用しているため、Mobile Access Security Gatewaysの導入に際してはSTA(Secure Ticketing Authority) サーバを使用する必要はありません。また、STAおよびCSG (Citrix Secure Gateway) サーバを使用した導入でも、Mobile Accessを使用できます。

Mobile Accessサーバの証明書には、Mobile Access Security GatewayのFQDNに対して発行されたFQDN(Fully Qualified Domain Name) を使用する必要があります。

Citrixサーバを使用したサンプルデプロイメント

これは、Mobile Access Security GatewayとCitrix Webサーバを DMZに配置した例です。Citrix XenAppサーバは、内部ネットワークに接続されています。



項目	説明
1	モバイルデバイス
2	モバイルアクセストンネル
3	インターネット (外部ネットワーク)
4	内部ネットワークのセキュリティゲートウェイ
5	DMZのモバイルアクセスセキュリティゲートウェイ
6	Citrix Webインタフェース
7	内部ネットワークリソース
8	Citrix XenApp (MetaFrame) サーバ

モバイルアクセス向けCitrixサービスの設定

この手順では、リモートユーザがCitrixアプリケーションに接続できるようにMobile Accessを設定する方法について説明します。このデプロイメントは、Citrixサーバを使用したサンプルデプロイメントに基づきます。*Citrixサーバを使用したサンプルデプロイメント (497ページ)*)。

Citrixサービスを設定するには

1. SmartConsoleで、**Manage & Settings > Blades**にアクセスします。
2. モバイルアクセスで、**Configure in SmartDashboard**をクリックします。
3. **Mobile Access** タブで、**Applications** >**Citrix Services** をクリックします。
4. **New**をクリックします。

   Citrix Serviceウィンドウの**General Properties**ページが開きます。
5. Citrixサーバオブジェクトの**Name**を入力します。
6. ナビゲーションツリーで**Web Interface**をクリックします。
7. Citrix Webインタフェースサーバーの新しいオブジェクトを作成します。**Servers** で、**Manage** >**New** >**Host** の順にクリックします。

   Host Nodeウィンドウが開きます。
8. Citrix Web Interfaceサーバの設定を入力します。
9. クリック**OK**。
10. Servicesで、Citrix Web Interfaceサーバでサポートされている次のサービスを1つまたは複数選択します。
    - HTTP
    - HTTPS
11. ナビゲーションツリーで**Link in Portal**をクリックします。
12. モバイルアクセスポータルでCitrixサービスへのリンクの設定を行います。
    - **Link text**- Citrixリンクに表示されるテキスト
    - **URL**- CitrixアプリケーションのディレクトリまたはサブディレクトリのURL。
    - **Tooltip**- Citrixリンクの上でマウスポインタを一時停止したときに表示されるテキスト
13. ナビゲーションツリーから、**Additional Settings** >**Single Sign On** を選択します。
14. Citrixサービスのシングルサインオンを有効にするには、以下のオプションを選択します。

- **Turn on single Sign On for this application**
- **Prompt users for their credentials, and store them for future use**

15. クリック**OK**。

    Citrixサーバオブジェクトは、**Defined Citrix Services**に追加されます。

16. Mobile Accessのナビゲーションツリーから、**Policy**を選択します。
17. 該当するルールにCitrixサービスオブジェクトを追加します。
    a. ルールのApplicationセルを右クリックし、**Add Applications**を選択します。
    b. Citrixサービスオブジェクトを選択します。
18. ポリシーをインストールします。

コンプライアンスチェック

Mobile Access Software Bladeでは、エンドポイントセキュリティオンデマンド機能を使用して、コンプライアンスポリシーを作成し、ネットワークにセキュリティを追加することができます。モバイルデバイスやコンピュータは、ネットワークに接続する前に一度スキャンされ、準拠しているかどうか確認します。

コンプライアンススキャナは、ActiveX(WindowsのInternet Explorerの場合) またはJavaを搭載したモバイルデバイスやコンピュータにインストールします。インターネットブラウザがモバイルアクセスポータルを開こうとすると、スキャンが開始されます。

コンプライアンスポリシー ルール

コンプライアンスポリシーは、さまざまな種類のルールで構成されています。各ルールに対してセキュリティとコンプライアンスに関する設定を行うか、デフォルトの設定を使用することができます。

これが、コンプライアンスポリシーのルールです。

- Windowsセキュリティ - Microsoft Windowsホットフィックス、パッチ、サービス パック。
- スパイウェア対策 - スパイウェア対策ソフト。
- ウィルス対策 - ウィルス対策ソフトのバージョンとウィルス署名ファイル。
- ファイアウォール - 個人用ファイアウォールソフト。
- スパイウェアスキャン - さまざまな種類のスパイウェアに対して行われるアクション。
- カスタム - アプリケーション、ファイル、登録キーなど、組織向けのコンプライアンスルール。
- ORグループ - 上記ルールのグループ。エンドポイントコンピュータがグループ内のルールの1つを満たしている場合、準拠していることになります。

コンプライアンスポリシーの作成

デフォルトでは、Endpoint Security on Demandは、コンプライアンスポリシーに準拠したエンドポイントコンピュータのみがMobile Access Portalにログインすることを許可します。

コンプライアンスポリシーを作成するには

1. SmartConsoleで、**Manage & Settings > Blades**にアクセスします。
2. モバイルアクセスセクションで、**Configure in SmartDashboard**をクリックします。
3. **Mobile Access**タブで、**Endpoint Security on Demand > Endpoint Compliance**を選択します。
4. **Edit policies**をクリックします。

   Policiesウィンドウが開きます。
5. **New Policy**をクリックします。

Policies > New Policyウィンドウが開きます。

6. ポリシーの**Name**と**Description**を入力します。
7. クリック**Add**。

   Add Enforcement Rulesウィンドウが開きます。

8. ポリシーのルールを選択します。

   新しいルールを作成することもできます。**New Rule**をクリックし、ルールの設定を行います。

9. クリック**OK**。

   Policies > New Policyウィンドウにポリシーのルールが表示されます。

10. 必要に応じて、**Bypass spyware scan**を選択してください。

    選択すると、アンチウィルスまたはアンチスパイウェアの設定に準拠したエンドポイントコンピュータのスキャンが変更されます。これらのコンピュータは、Mobile Access Security Gatewayに接続する際にスパイウェアのスキャンを行いません。

11. クリック**OK**。

    Policiesウィンドウが開きます。

12. クリック**OK**。

セキュリティゲートウェイのコンプライアンスの設定

モバイルアクセスセキュリティゲートウェイ上のファイアウォールは、コンプライアンスポリシーに準拠したエンドポイントコンピュータへのアクセスのみを許可します。

この手順では、セキュリティゲートウェイにラップトップコンピュータポリシーを設定する方法を示します(*コンプライアンスポリシールール (500ページ)*)。

コンプライアンス設定を行うには

1. SmartConsoleで、**Manage & Settings > Blades**にアクセスします。
2. **Mobile Access**セクションで、**Configure in SmartDashboard**をクリックします。
3. **Mobile Access**タブで、**Endpoint Security on Demand > Endpoint Compliance**を選択します。
4. セキュリティ」を選択し、**Edit**をクリックします。

   セキュリティゲートウェイのプロパティウィンドウの**Endpoint Compliance**ページが表示されます。

5. **Scan endpoint machine when user connects**を選択します。
6. **Threshold policy**を選択し、ドロップダウンメニューから**Laptop Computer**を選択します。

7. クリックOK。
8. モバイルアクセスセキュリティゲートウェイにポリシーをインストールします。

Secure Workspace

Secure Workspaceは、リモートユーザが企業のネットワークリソースに安全かつ確実に接続できるようにするセキュリティソリューションです。仮想ワークスペースであるSecure Workspaceは、実際のワークスペースとは分離されたセキュアな環境をエンドポイントコンピュータ上に提供します。ユーザは、このセキュアな環境から、Mobile Access Portalを通じてのみデータを送信することができます。Secure Workspaceのユーザは、仮想ワークスペースから許可されたアプリケーション、ファイル、およびその他のリソースにのみアクセスすることができます。

Secure Workspaceは、コンピュータ上にMy Secured Documentsという暗号化されたフォルダを作成し、仮想デスクトップからアクセスできるようにします。このフォルダには、ユーザが一時的に保存するファイルが格納されます。セッションが終了すると、Secure Workspaceでこのフォルダとその他のすべてのセッションデータが削除されます。

Secure Workspace および Mobile Access VPNの設定の詳細については、以下を参照してください。*R82 Mobile Access Administration Guide*。

モバイルアクセスセキュリティゲートウェイでSecure Workspaceを有効にするには

1. SmartConsoleで、**Manage & Settings > Blades**にアクセスします。
2. **Mobile Access**セクションで、**Configure in SmartDashboard**をクリックします。

   レガシーSmartDashboardが開きます。
3. **Mobile Access** タブで、**Endpoint Security on Demand >Secure Workspace** をクリックします。
4. セキュリティゲートウェイを選択し、**Edit**をクリックします。

   セキュリティゲートウェイのプロパティウィンドウの**Check Point Secure Workspace**ページが表示されます。
5. **This gateway supports access to applications from within Check Point Secure Workspace**を選択します。
6. クリックOK。
7. ポリシーをインストールします。

Secure Workspace

Secure Workspaceは、リモートユーザが企業のネットワークリソースに安全かつ確実に接続できるようにするセキュリティソリューションです。仮想ワークスペースであるSecure Workspaceは、実際のワークスペースとは分離されたセキュアな環境をエンドポイントコンピュータ上に提供します。ユーザは、このセキュアな環境から、Mobile Access Portalを通じてのみデータを送信することができます。Secure Workspaceのユーザは、仮想ワークスペースから許可されたアプリケーション、ファイル、およびその他のリソースにのみアクセスすることができます。

Secure Workspaceは、コンピュータ上に**My Secured Documents**という暗号化されたフォルダを作成し、仮想デスクトップからアクセスできるようにします。このフォルダには、ユーザが一時的に保存するファイルが格納されます。セッションが終了すると、Secure Workspaceでこのフォルダとその他のすべてのセッションデータが削除されます。

Secure Workspace および Mobile Access VPN の設定の詳細は、以下を参照してください。*R82 Mobile Access Administration Guide*。

モバイルアクセスセキュリティゲートウェイでSecure Workspaceを有効にするには

1. SmartConsoleで、**Manage & Settings > Blades**にアクセスします。
2. **Mobile Access**セクションで、**Configure in SmartDashboard**をクリックします。

   レガシーSmartDashboardが開きます。
3. **Mobile Access** タブで、**Endpoint Security on Demand** >**Secure Workspace** をクリックします。
4. セキュリティゲートウェイを選択し、**Edit**をクリックします。

   セキュリティゲートウェイのプロパティウィンドウの**Check Point Secure Workspace**ページが表示されます。
5. **This gateway supports access to applications from within Check Point Secure Workspace**を選択します。
6. クリック**OK**、そしてポリシーをインストールします。

モバイルアクセスについての詳 細

Mobile Access VPNの詳 細については、次を参 照してください。*R82 Mobile Access Administration Guide*。

サイト間VPN

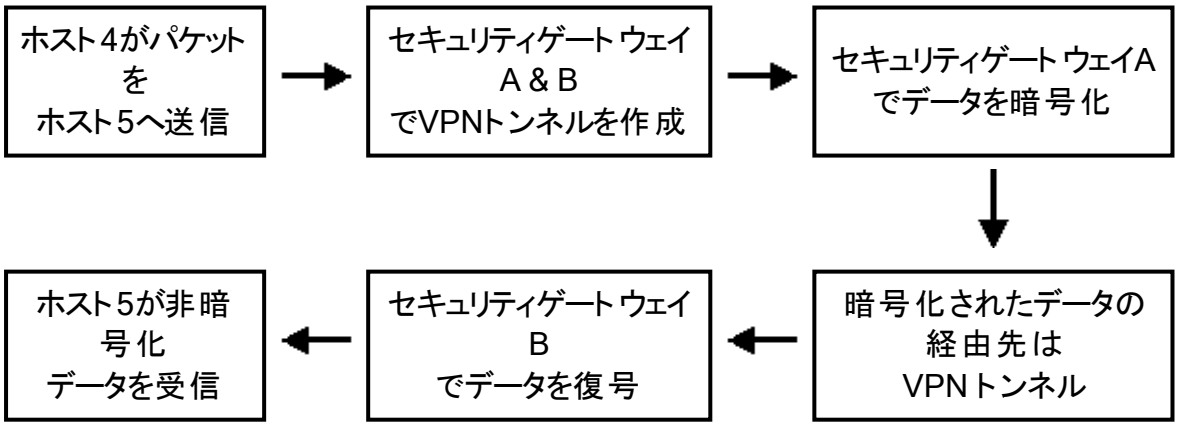
サイト間VPNの基本は、暗号化されたVPNトンネルです。2台のセキュリティゲートウェイがリンクをネゴシエートしてVPNトンネルを作成し、各トンネルに複数のVPN接続を含めることができます。1台のセキュリティゲートウェイは、同時に複数のVPNトンネルを維持することができます。

サイト間VPNの導入例

項目	説明
A、B	セキュリティゲートウェイ
2	VPNトンネル
3	VPNドメインの内部ネットワーク
4	ホスト4
5	ホスト5

この例のVPN展開では、ホスト 4 とホスト 5 が相互にデータを安全に送信しています。セキュリティゲートウェイはIKEネゴシエーションを行い、VPNトンネルを作成します。ホスト4とホスト5の間で送信されるデータの暗号化と復号にIPsecプロトコルを使用しています。

VPNワークフロー

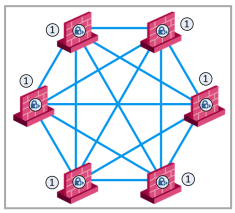


VPNコミュニティ

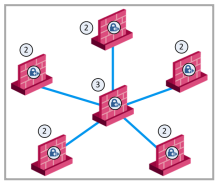
VPNドメインとは、VPNトラフィックを送受信するためにセキュリティゲートウェイを使用する内部ネットワークの集合です。各セキュリティゲートウェイのVPNドメインに含まれるリソースを定義します。次に、セキュリティゲートウェイをVPNコミュニティ(VPNトンネルとその属性の集合) に参加させます。異なるVPNドメインのネットワークリソースは、VPNコミュニティ内のセキュリティゲートウェイを終端とするVPNトンネルを通じて、互いに安全に通信することができます。

VPNコミュニティは、スター型とメッシュ型のトポロジをベースにしています。メッシュコミュニティでは、各セキュリティゲートウェイのペアの間にVPNトンネルが存在します。スターコミュニティでは、各サテライトセキュリティゲートウェイはセントラルセキュリティゲートウェイへのVPNトンネルを持ちますが、コミュニティ内の他のセキュリティゲートウェイへのVPNトンネルは持ちません。

Mesh Topology



Star Topology



項目	説明
1	セキュリティゲートウェイ
2	サテライト セキュリティ ゲートウェイ
3	セントラルセキュリティゲートウェイ

サンプルスターのデプロイメント

VPNスターコミュニティの設定方法について説明します。この配置では、サテライトセキュリティゲートウェイがセントラルセキュリティゲートウェイの内部ネットワークに接続することができます。内部ネットワークオブジェクトの名前は、**Internal-network**です。

VPN スターコミュニティを新規に作成するには

1. SmartConsoleで、**Security Policies**ページにアクセスします。
2. **Access Tools**セクションで、**VPN Communities**をクリックします。
3. **New**をクリックし、**Star Community**を選択します。

   New Star Communityウィンドウが開きます。
4. コミュニティの名前を入力します。
5. ナビゲーションツリーで、**Encryption**を選択します。
6. VPNコミュニティのVPN暗号化方式とアルゴリズムを設定します。
7. クリック**OK**。

セキュリティゲートウェイにスター型VPNを設定するには

VPNコミュニティ内の各セキュリティゲートウェイについて、以下の設定手順を実行します。

1. SmartConsoleで、**Gateways & Servers**ページに移動し、セキュリティゲートウェイオブジェクトをダブルクリックします。

   セキュリティゲートウェイのプロパティ画面が表示されます。

2. **General Properties**ページの**Network Security**セクションで、**IPsec VPN**を選択します。
3. ナビゲーションツリーで**Network Management > VPN Domain**をクリックします。
   - 中央のセキュリティゲートウェイの場合、**Manually defined**をクリックし、**Internal-network**オブジェクトを選択します。
   - サテライトセキュリティゲートウェイの場合、**All IP addresses**
4. ナビゲーションツリーで**IPsec VPN**をクリックします。
5. セキュリティゲートウェイをVPNスターコミュニティのメンバとして設定します。
   a. **This Security Gateway participates in the following VPN Communities**セクションで、**Add**をクリックします。

      Add this Gateway to Communityウィンドウが開きます。

   b. VPNコミュニティを選択します。
   c. クリック**OK**。
6. クリック**OK**。

コミュニティを作成し、セキュリティゲートウェイを設定した後、それらのセキュリティゲートウェイをセンターまたはサテライトセキュリティゲートウェイとしてコミュニティに追加します。

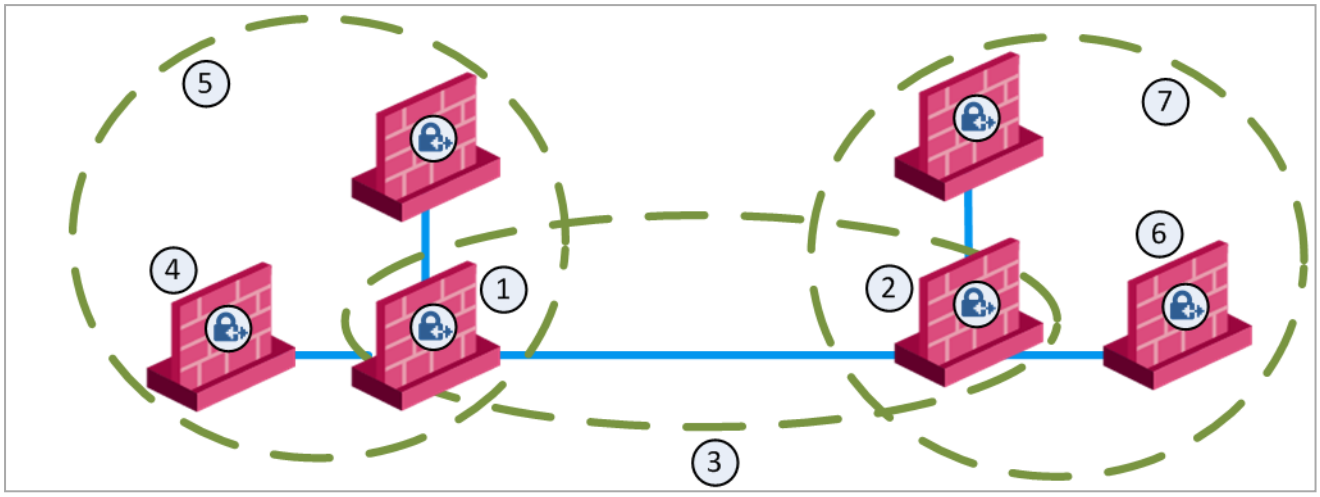
セキュリティゲートウェイを新しいスターコミュニティに追加するには

1. SmartConsoleで、**Security Policies**ページにアクセスします。
2. **Access Tools**セクションで、**VPN Communities**をクリックします。
3. 新しいスターコミュニティを選択し、**Edit**をクリックします。

   Star Communityウィンドウが開きます。

4. **Gateways**ページで、セキュリティゲートウェイをコミュニティに追加します。
   - **Center Gateways- Add**をクリックし、centerセキュリティゲートウェイを選択します。必要に応じて、**Mesh center gateways**を選択します。
   - **Satellite Gateways- Add**をクリックし、サテライトセキュリティゲートウェイを選択します。
5. クリック**OK**。

VPNコミュニティの組合せ例



項目	説明
1	ロンドン セキュリティゲート ウェイ
2	ニューヨーク セキュリティゲート ウェイ
3	ロンドン-ニューヨーク メッシュコミュニティ
4	ロンドンの企業パートナー(外部ネットワーク)
5	ロンドン スターコミュニティ
6	ニューヨークの企業パートナー(外部ネットワーク)
7	ニューヨークスターコミュニティ

この導入では、内部ネットワークを共有するロンドンとニューヨークのセキュリティゲート ウェイのMeshコミュニティで構成されています。パートナー企業の外部ネットワーク用セキュリティゲート ウェイは、ロンドン、ニューヨークの内部ネットワークにはアクセスできません。しかし、スターVPNコミュニティでは、企業のパートナーが協力する拠点の内部ネットワークにアクセスすることができます。

VPN接続の許可

特定のVPNコミュニティ内のセキュリティゲート ウェイ間のVPN接続を許可するには、対象接続を受け入れるアクセスコントロールルールを追加します。

特定のVPNコミュニティの内部ネットワーク上のホストおよびクライアントに対するすべてのVPNトラフィックを許可するには、そのVPNコミュニティのプロパティ設定ウィンドウの**Encrypted Traffic**のセクションでこれらのオプションを選択します。

- メッシュ化されたコミュニティ: **Accept all encrypted traffic**
- スターコミュニティ: **Accept all encrypted traffic on Both center and satellite gateways**または**Accept all encrypted traffic on Satellite gateways only**。

VPNアクセスコントロールルールのサンプル

この表は、アクセスコントロールルールベースのVPNルールのサンプルを示します。(**Action**、**Track**、**Time**のカラムは表示されていません。**Action**は**Allow**に、**Track**は**Log**に、**Time**は**Any**に設定されています)。

No.	名前	発信元	宛先	VPN	サービス	インストール先
1	-	Any	**NEGATED**メンバセキュリティゲートウェイ	BranchOffices LondonOffices	Any	BranchOffices LondonOffices
2	サイト間VPN	Any	Any	All_GwToGw	FTP-port HTTP HTTPS SMTP	ポリシーの対象
3	リモートアクセス	Any	Any	RemoteAccess	HTTP HTTPS IMAP	ポリシーの対象

1. `BranchOffices` VPNコミュニティおよび`LondonOffices` VPNコミュニティで**Accept All Encrypted Traffic**設定オプションが選択されている場合に、SmartConsoleが*暗黙のルール*の最上位に追加する自動ルール。このルールは、これらのコミュニティ内のすべてのセキュリティゲートウェイにインストールされます。これらのコミュニティの内部ネットワーク上のホストやクライアントへのすべてのVPNトラフィックを許可します。これらのVPNコミュニティ内のセキュリティゲートウェイに送信されたトラフィックはドロップされます。

   注 - この自動ルールは、複数のVPNコミュニティに適用することができます。

2. **Site-to-site VPN**- すべてのSite-to-Site VPNコミュニティのVPNドメイン内のホスト間の接続が許可されます。許可されるプロトコルはFTP、HTTP、HTTPS、SMTPだけです。
3. **Remote access**- リモートアクセスVPNコミュニティのVPNドメイン内のホスト間の接続は許可されます。許可されるプロトコルは、HTTP、HTTPS、IMAPだけです。

サイト間VPNについての詳細

サイト間VPNの詳細については、以下を参照してください。*R82 Site to Site VPN Administration Guide*。

リモート アクセス VPN

従業員がさまざまな場所やデバイスから機密情報にリモートアクセスする場合、システム管理者はこのアクセスがセキュリティ上の脆弱性にならないようにする必要があります。Check Pointのリモートアクセス VPN ソリューションを使用すると、リモートユーザと内部ネットワークとの間にVPNトンネルを構築することができます。Mobile Access Software Bladeは、リモートアクセスソリューションの機能を拡張し、多くのクライアントや導入を可能にします。

VPN接続モード

リモートクライアントが社内リソースを安全に接続する際、企業は次のような接続の課題に直面します。

- リモートアクセスクライアントのIPアドレスが不明な場合がある
- リモートアクセスクライアントが内部IPアドレスを持つLANに接続する(ホテルなど)
- リモートクライアントでサポートされていないプロトコルを使う必要がある

Check Point IPsec VPN Software Blade は、このような課題を解決するために、以下のVPN接続モードを提供します。

- **オフィスモード**

  リモートユーザには、ローカルISPから同一または非ルーティングIPアドレスを割り当てることができます。オフィスモードは、これらのルーティングの問題を解決し、内部ネットワークから利用可能なIPアドレスでIPパケットをカプセル化します。リモートユーザは、オフィスにいるのと同じようにトラフィックを送信でき、VPNルーティングの問題を回避することができます。

- **ビジタモード**

  リモートユーザは、HTTPとHTTPSのプロトコルのみを使用するように制限することができます。ビジターモードでは、これらのユーザがポート443の通常のTCP接続を通じて、すべてのプロトコルをトンネリングすることができます。

リモートアクセスVPNワークフローの例

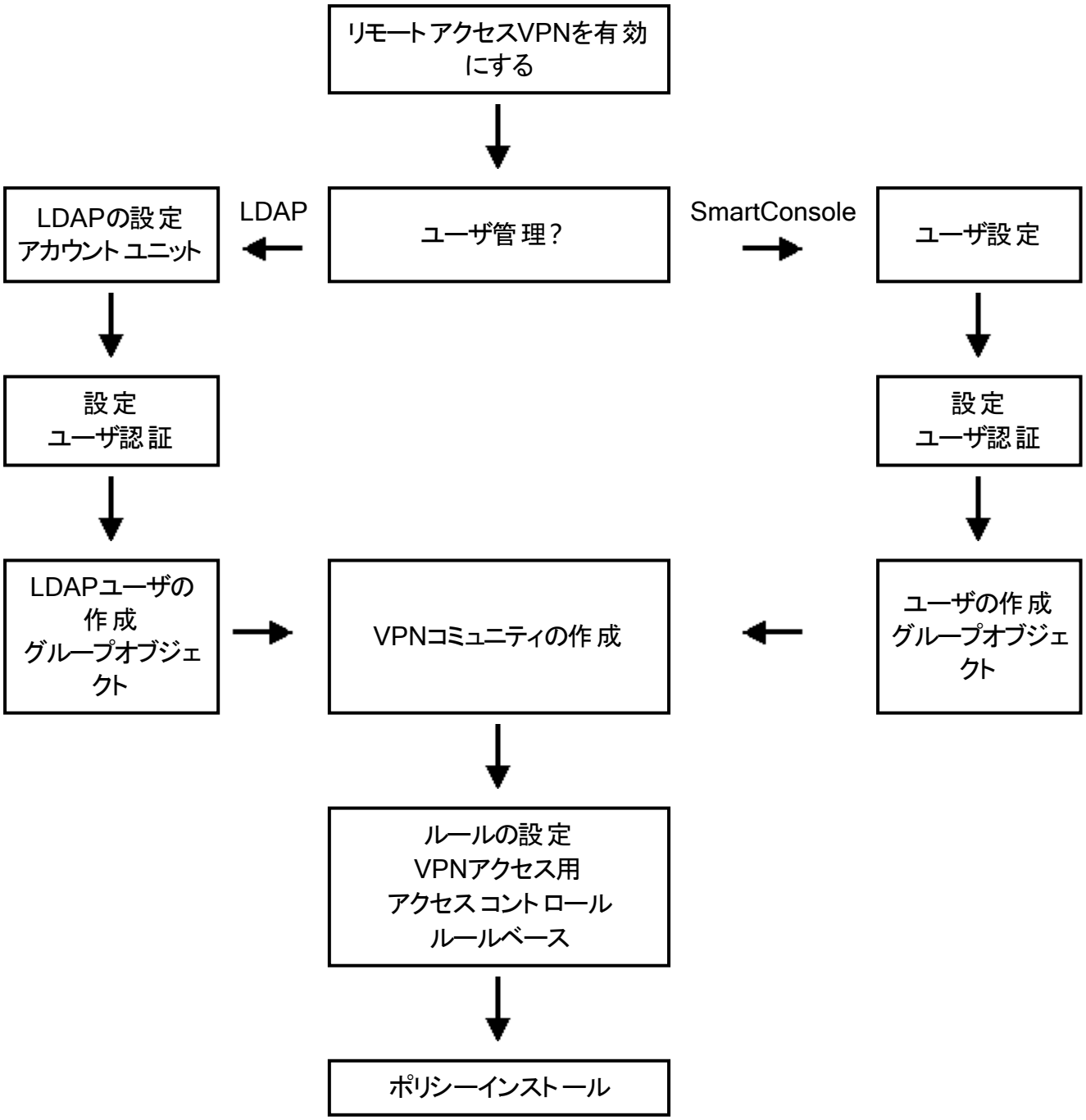
以下は、リモートアクセスVPNのワークフローの例です。

1. SmartConsoleを使用して、Security GatewayでRemote Access VPNを有効にします。
2. Security Management Serverにリモートユーザの情報を追加します。
   - LDAPアカウントユニットの作成と設定
   - SmartConsoleのユーザデータベースに情報を入力します。

   オプション:リモートユーザ認証用にセキュリティゲートウェイを設定します。
3. セキュリティゲートウェイのアクセスコントロールと暗号化ルールを定義します。
4. Security Gatewayのルールで使用するグループオブジェクトを作成します。

- **LDAP Group**オブジェクト - LDAP アカウント ユニット の場 合
- **User Group**オブジェクト - SmartConsole ユーザデータベースに設 定されたユーザ用

5. **Menu** >**Global properties** >**Remote Access** >**VPN - Authentication and Encryption** に VPNコミュニティオブジェクト の暗 号 化 設 定 を作 成し、設 定します。
6. アクセスコント ロールルールベースにアクセスコント ロールルールを追 加し、内 部 ネット ワークへのVPNト ラフィックを許 可します。



リモート アクセスコミュニティのセキュリティゲート ウェイの設 定

リモート アクセスコミュニティを設 定 する前 に、VPN Software Bladeが有 効 になっていることを確 認 してください。

リモート アクセス用 セキュリティゲート ウェイを設 定 するには

1. SmartConsoleで、**Gateways & Servers**をクリックし、セキュリティゲート ウェイをダブルクリックします。

   Security Gatewayオブジェクト が開き、**General Properties**ページが表 示 されます。

2. ナビゲーションツリーで**IPsec VPN**をクリックします。

   セキュリティゲート ウェイが参 加 しているVPNコミュニティが表 示 されます。

3. リモート アクセスコミュニティにセキュリティゲート ウェイを追 加 するには:

   a. クリック**Add**。

   b. コミュニティを選 択 します。

   c. クリック**OK**。

4. ナビゲーションツリーで**Network Management > VPN Domain**をクリックします。

5. VPNドメインを設 定 します。

ビジタモード の設 定 を行うには

1. ナビゲーションツリーで**VPN Clients > Office Mode**をクリックします。

2. オフィスモード の設 定 を行 います。

   注 - オフィスモード のサポート は、セキュリティゲート ウェイ側 で必 須 です。

3. クリック**OK**。

4. SmartConsoleセッションを公 開 する。

リモート アクセスVPNについて

詳 細 は*R82 Remote Access VPN Administration Guide*。

暗黙のルール

Check Point Security Management Serverとその管理対象オブジェクト(セキュリティゲートウェイ、クラスタメンバ、ログサーバなど)は、Check Pointのプロトコルを介して相互に通信します。デフォルトでは、各アクセスコントロールポリシーには、Check Point内部での必要な通信を許可する、事前に定義された暗黙のルールが含まれています。

SmartConsoleで暗黙のルールを表示するには:

1. 左のナビゲーションパネルから、Security Policiesをクリックします。
2. 左上のパネルで、Access Control > **Policy** をクリックします。
3. 上部のツールバーから、**Actions** >**Implied Rules** をクリックします。

SmartConsoleで暗黙のルールを設定するには:

1. 左上隅から、**Menu** > **Global properties**をクリックします。
2. **Firewall**ページで、該当するオプションを選択し、暗黙のルールの順序を設定します。
3. クリック**OK**
4. 管理対象の各セキュリティゲートウェイ/クラスタ/仮想システムにアクセス制御ポリシーをインストールします。

詳細は、sk179346を参照してください。

新しい脅威対策ポリシーの作成

脅威対策ポリシーの設定については、以下を参照してください。*R82 Threat Prevention Administration Guide*。

脅威対策ポリシーのインストール

IPS、Anti-Bot、Anti-Virus、Threat Emulation、Threat Extraction Software Bladesには、専用の脅威対策ポリシーがあります。このポリシーは、Access Control Software Bladeのポリシーのインストールとは別にインストールできます。セキュリティゲートウェイのパフォーマンスへの影響を最小限に抑えるため、脅威対策ポリシーのみをインストールします。

脅威対策ポリシーをインストールするには

1. グローバルツールバーから**Install Policy**をクリックします。

   Install Policyウィンドウが開き、インストール先(Security Gateways)が表示されます。

2. **Threat Prevention**を選択します。
3. 選択**Install Mode:**

   - **Install on each selected gateway independently**- 他のターゲットを参照せずに、選択したセキュリティゲートウェイにポリシーをインストールします。あるセキュリティゲートウェイへのインストールに失敗しても、他のセキュリティゲートウェイへのポリシーインストールには影響しません。

     セキュリティゲートウェイがクラスタのメンバである場合は、すべてのメンバにポリシーをインストールします。Security Management Serverは、すべてのメンバにポリシーをインストールできることを確認してから、いずれかのメンバにポリシーをインストールします。1つのメンバにポリシーをインストールできない場合、すべてのメンバに対してポリシーのインストールに失敗します。

   - **Install on all selected gateways, if it fails do not install on gateways of the same version**- すべてのインストールターゲットにポリシーをインストールします。ポリシーのインストールに失敗した場合、ポリシーは同じバージョンの他のターゲットにはインストールされません。

4. クリック**OK**。

脅威の分析

今日のネットワークは、かつてないほどサイバー脅威にさらされています。これは、組織にとって、セキュリティ上の脅威を理解し、被害を評価する上での課題となっています。

SmartConsoleは、セキュリティ管理者がサイバー脅威の原因を見つけ、ネットワークを修復するのに役立ちます。

Logs & Events > **Logs**ビューでは、脅威がログとして表示されます。

Logs & Eventsビューの他のビューは、ログを意味のあるセキュリティイベントにまとめられます。例えば、選択した時間間隔(直近の1時間、1日、1週間、1ヶ月)にネットワーク内のホストで発生した悪意のあるアクティビティ。また、感染前後の統計も示します。

ログとイベントモニタ用の豊富でカスタマイズ可能なビューとレポートを作成し、主要な関係者にセキュリティ活動を知らせることができます。各ログやイベントに対して、マルウェア、ウイルス、攻撃に関するThreatWikiやIPS Advisoriesから多くの有用な情報を見ることができます。

詳細:

- *R82 Threat Prevention Administration Guide*。
- *R82 Logging and Monitoring Administration Guide*。

アクセスコントロールポリシーのUserCheck

このセクションでは、UserCheck の設定と使用方法について説明します。

UserCheck機能を有効にすると、管理者がセキュリティポリシーで設定したルールに基づいて、セキュリティゲートウェイは、コンプライアンスに違反する可能性のある行動や危険なインターネット閲覧に関するメッセージをユーザに送信します。これは、セキュリティインシデントを防ぎ、組織のセキュリティポリシーを学ぶために役立ちます。ログに記録されたユーザの反応に基づいて、効果的なポリシーを策定することができます。UserCheckオブジェクトを作成し、ルールベース内で使用して、ユーザと通信します。

これらのSoftware Bladeは、UserCheck機能をサポートしています:

- DLP (データ損失防止)
- アクセスコントロール:
  - アプリケーション コントロール
  - URL フィルタリング
  - コンテンツアウェアネス
- 脅威対策:
  - アンチボット
  - アンチウイルス
  - Threat Emulation
  - Threat Extraction
  - ゼロフィッシング

Data Loss Prevention Software BladeのUserCheckの使用:

詳細は*R82 Data Loss Prevention Administration Guide*> UserCheckの章

Application Control、URL Filtering、Content Awareness Software BladesのUserCheckの使用：

1. SmartConsoleで、セキュリティゲートウェイ / クラスタオブジェクトを開きます：
   a. 該当するAccess Control Software Bladesを有効にします。
   b. 該当するUserCheckの設定を行います。
      参照：*UserCheckの設定 (518ページ)*。
   c. オプション：UserCheck Clientをダウンロードし、エンドポイントコンピュータにインストールします。
      詳細は*R82 Quantum Security Gateway Guide*> UserCheckクライアントの章
2. オプション：**Global Properties**で、該当するUserCheckアプリケーション設定を行います。
3. 該当する UserCheck インタラクションオブジェクトを設定します。
   参照：*Access Control Software BladesのUserCheckインタラクションオブジェクト (522ページ)*。
4. 該当するアクセスコントロールポリシーを設定します。
   参照：*アクセスコントロールポリシーの作成 (326ページ)*:
   アクセスコントロールルールで、**Action**カラムをクリック > 該当するメニュー**Drop**、**Ask**、または**Inform**をクリック > 必要な UserCheck Interaction オブジェクトを選択します。
5. セキュリティゲートウェイ/クラスタオブジェクトにアクセスコントロールポリシーをインストールします。
6. 追加設定：
   - *UserCheck ポータルのローカライズとカスタマイズ (530ページ)*

UserCheckの設定

セキュリティゲートウェイでUserCheckを直接有効または無効にします。UserCheckが有効な場合、ユーザのインターネットブラウザの新しいウィンドウで、UserCheckメッセージが表示されます。ユーザがリモートでセキュリティゲートウェイに接続する場合、セキュリティゲートウェイの内部インタフェース(**Topology**ページ) をUserCheck Portalの**Main URL**と同じに設定します。

セキュリティゲートウェイでUserCheckを構成する手順

ステップ	手順
1	左側のナビゲーションパネルで**Gateways & Servers**をクリックします。
2	セキュリティゲートウェイ / クラスタオブジェクトをダブルクリックします。
3	左のパネルで、UserCheckをクリックします。
4	**Enable UserCheck for active blades**を選択します。
5	**UserCheck Web Portal**セクションの**Main URL**フィールドには、UserCheck通知を表示するWebポータルのプライマリURLが表示されます。 提案された**Main URL**を使用するか、手動で別の**Main URL**を入力することができます。
6	オプションです。 異なるホスト名を**Aliases**にリダイレクトするURLエイリアスを追加するには、**Main URL**をクリックします。 例：`usercheck.mycompany.com` エイリアスは、企業DNSサーバ上のポータルIPアドレスに解決される必要があります。
7	**Certificate**セクションで「**Import** 」をクリックして、ポータルがSecurity Management Serverへの認証に使用する証明書をインポートします。 デフォルトでは、ポータルはCheck Point内部認証局(ICA) の証明書を使用します。 このため、ユーザのブラウザがCheck Pointを信頼できる認証局として認識していない場合、警告が表示されることがあります。 警告を防ぐには、公認の外部機関から独自の証明書をインポートすることが重要です。 **注** - 証明書をダウンロードした後、**Replace**をクリックして別の証明書に置き換え、**View**をクリックして証明書情報を見ることができます。

ステップ	手順
8	**Accessibility**セクションで、**Edit**をクリックして、ポータルにアクセスできるセキュリティゲートウェイのインタフェースを設定します。 これらのオプションは、セキュリティゲートウェイオブジェクトで設定されたトポロジーに基づいています。 **Network Managment**ページでトポロジ設定を行います。 セキュリティゲートウェイが、接続方法に基づいてユーザをUserCheckポータルに送信する必要がある場合は、該当するオプションを選択します: ■ **Through all interfaces** ■ **Through internal interfaces**(デフォルト) • **Including undefined internal interfaces** • **Including DMZ internal interfaces** • **Including VPN encrypted interfaces**(デフォルト) ルートベースVPNトンネル(VTI) の確立に使用されるインタフェースに適用 ■ **According to the Firewall Policy** UserCheckポータルにアクセスできるユーザを決定するアクセス制御ルールがある場合は、このオプションを選択します。 **Main URL**が外部インタフェースに設定されている場合、**Accessibility**のいずれかに設定する必要があります: ■ **Through all interfaces** VSXゲートウェイ / VSXクラスタの場合は、このオプションを選択する必要があります。 ■ **According to the Firewall Policy**
9	**UserCheck Client**- UserCheck Clientは、セキュリティゲートウェイと通信し、UserCheck Interaction通知をユーザに表示するために、ユーザのデバイスにインストールされます。 ■ **Activate UserCheck Client support** これにより、UserCheck Clientを介したUserCheckが有効になります。 ■ **Download Client** UserCheck Clientのインストールファイルをダウンロードします。 **注** - リンクは、UserCheckポータルが立ち上がるまで有効ではありません。 詳細は*R82 Quantum Security Gateway Guide*> UserCheckクライアントの章

<table>
<tr><th>ステップ</th><th>手順</th></tr>
<tr><td>10</td><td>Mail Serverセクションで、UserCheck 用のメールサーバを設定します。
このサーバは、サーバがユーザのEメールアドレスを知っている場合、セキュリティゲートウェイが他の手段で通知できないユーザに通知を送信します。
たとえば、ユーザがルールに一致するEメールを送信した場合、トラフィックがHTTPではないため、セキュリティゲートウェイはユーザをUserCheck Portalにリダイレクトできません。
ユーザがUserCheck Clientを持っていない場合、UserCheckはユーザにEメール通知を送信します。

■ Use the default settings
リンクをクリックして、どのメールサーバが設定されているかを確認します。
■ Use specific settings for this gateway
デフォルトのメールサーバ設定を上書きするには、このオプションを選択します。
■ Send emails using this mail server
リストからメールサーバを選択するか、Newをクリックして新しいメールサーバを定義します。</td></tr>
<tr><td>11</td><td>クリックOKセキュリティゲートウェイ / クラスタオブジェクトを閉じます。</td></tr>
<tr><td>12</td><td>内部インタフェース経由の暗号化トラフィックがある場合、アクセスコントロールポリシーのファイアウォールレイヤに新しいルールを追加します。
ルールの例：
<table>
<tr><th>発信元</th><th>宛先</th><th>VPN</th><th>サービス&アプリケーション</th><th>アクション</th></tr>
<tr><td>Any</td><td>セキュリティゲートウェイ
UserCheckクライアント
有効</td><td>Any</td><td>UserCheck</td><td>承認</td></tr>
</table>
</td></tr>
</table>

ステップ	手順
13	アクセスコントロールポリシーをインストールして、これらのAccess Control Software BladesのUserCheckを有効にします。 ■ アプリケーション コントロール ■ URL フィルタリング ■ コンテンツアウェアネス ■ DLP (データ損失防止) 脅威対策ポリシーをインストールして、Threat Prevention Software BladesのUserCheckを有効にします: ■ アンチボット ■ アンチウイルス ■ Threat Emulation ■ Threat Extraction ■ ゼロフィッシング

UserCheck CLI

詳細は*R82 CLI Reference Guide*- セキュリティゲートウェイのコマンド "の章 - "usrchk "のセクション。

Access Control Software BladesのUserCheckインタラクションオブジェクト

ここでは、UserCheck インタラクションオブジェクトの設定方法について説明します。

UserCheck インタラクションオブジェクトは、柔軟性を追加し、セキュリティゲートウェイにユーザと通信するメカニズムを与えます。

アクセスコントロールポリシーの「**Action**」カラムにある「UserCheck Interaction Objects」は、以下のように使用します:

- 組織のセキュリティに対して危険な決断を下すユーザの支援。
- Webアプリケーションやサイトのインターネットポリシーを変更する組織をリアルタイムでユーザと共有。

注 - Access ControlポリシーのUserCheckインタラクションオブジェクトは、SmartConsoleでのみ作成および編集できます。

UserCheckインタラクションのアクションタイプ

アクションタイプ	説明
Ask	ユーザは、リクエストしたサイトに進むかどうかを尋ねるメッセージを受け取る。 このアクションタイプを持つUserCheckインタラクションは、アクセスコントロールルールのプロファイル >**Action** カラムをクリック > すると、メニュー**Ask**に表示されます。
Block	ユーザには、会社のポリシーによってリクエストサイトへのアクセスがブロックされているというメッセージが表示されます。 このアクションタイプを持つUserCheckインタラクションは、アクセスコントロールルールのプロファイル >**Action** カラムをクリック > すると、メニュー**Drop**に表示されます。
Cancel	ユーザが**Inform**または**Ask**通知を受け取り、**Cancel**をクリックすると、サイトへのアクセス要求をキャンセルしたというメッセージが表示されます。
Inform	ユーザはリクエストしたサイトの企業ポリシーに関するメッセージを受け取り、サイトに進むには**OK**をクリックする必要があります。

アクセスコントロールのためのデフォルトのUserCheckインタラクションオブジェクト

説明

注：

- これらのデフォルトのオブジェクトは、読み取り専用ビューで開きます。
- 各デフォルトオブジェクトを右クリックし、**Clone**をクリックします。
- デフォルトの UserCheck インタラクションオブジェクトをプレビューするには、そのオブジェクトをクリックします。

1. 左側のナビゲーションパネルで**Security Policies**をクリックします。
2. 上部パネルで、**Access Control**をクリックします。
3. 下のパネルで、**Access Tools**をクリックし、**UserCheck**をクリックする。
4. これらは、アクセスコントロールのデフォルトの UserCheck インタラクションオブジェクトです：

デフォルトの UserCheck インタラクションオブジェクト	アクションタイプ
Company Policy	Ask
Blocked Message - Access Control	Block
Cancel Page - Access Control	Cancel
Access Approval	Inform
Access Notification	Inform

アクセスコントロールのための新しいUserCheck相互作用オブジェクトの作成

手順

1. 左側のナビゲーションパネルで**Security Policies**をクリックします。
2. 上部パネルで、**Access Control**をクリックします。
3. 下のパネル**Access Tools**で、**UserCheck**をクリックします。
4. 上部のツールバーから、**New** > 該当する UserCheck Interaction をクリックします：

   注 - デフォルトのUserCheck Interactionオブジェクトを右クリックし、[**Clone**] をクリックすると、必要に応じてクローン化されたオブジェクトを編集できます。

- **Ask UserCheck**

  該当するSoftware Bladeの脅威対策プロファイルでこのUserCheck Interactionオブジェクトを選択すると、内部ユーザには要求を続行するかどうかを尋ねるメッセージが表示されます。

  リクエストを続行するには、理由を入力します。

- **Inform UserCheck**

  該当するSoftware Bladeの脅威対策プロファイルでこのUserCheck Interactionオブジェクトを選択すると、内部ユーザに情報メッセージが表示されます。

  ユーザはリクエストを続行またはキャンセルすることができます。

- **Block UserCheck**

  該当するSoftware Bladeの脅威対策プロファイルでこのUserCheck Interactionオブジェクトを選択すると、内部ユーザにはリクエストがブロックされたというメッセージが表示されます。

5. **オプション:** 上部の隅、アイコンの右側にある下向きの矢印をクリックし、希望の色を選択します。
6. 一番上のフィールドに、オブジェクト名を入力します。
7. **オプション:** **Comment**フィールドに、該当するテキストを入力します。
8. 左のパネルで、**Message**ページをクリックします:
   a. メッセージの言語を選択するには(デフォルトは英語) 、メッセージセクションの上にある**Languages**ボタンをクリック > 必要な言語を選択 >**OK**をクリックします。

      注 - 選択した言語ごとに対応するタブが表示されます。

   b. 変数フィールドをメッセージに挿入するには、上部のツールバーから**Insert Field**をクリックし、該当する変数をクリックします。

      注:
      - **Ask**、**Inform**、または**Block**アクションが発生すると、UserCheck PortalおよびUserCheckクライアントアプリケーションは、これらの変数をメッセージ内の該当する値に置き換えます。
      - **Username**変数を解決するには、**Identity Awareness** Software Bladeを有効にし、必要な設定を行う必要があります。詳細は*R82 Identity Awareness Administration Guide*。

c. ロゴを追加するには、メッセージ本文で**Add Logo**をクリック > ✳をクリック > **Add new image**をクリック > 必要な画像ファイルを参照して選択 > **Open**をクリックします。

注
- 画像の高さは176ピクセル以下です。
- 画像の幅は52ピクセル以下です。

d. ユーザ入力用の特別なフィールドを挿入するには、上部のツールバーから**Insert User Input**をクリックし、該当するオプションをクリックします。

重要:
- 生のHTMLコードに表示を変更するには、上部の**Source**をクリックします。
  戻るには**Design**をクリックします。
- このオブジェクトの保存後、最終的なメッセージをプレビューできます。

9. 左のパネルで、**Settings**ページをクリック:

a. **Languages**セクションで:

ユーザがWebブラウザでデフォルト言語を設定していない場合、UserCheckページの言語を選択します。

b. **Faillback Action**セクションで:

注 - このセクションは、**Ask**および**Inform**タイプのUserCheck Interactionオブジェクトにのみ表示されます。

ユーザのコンピュータにUserCheck通知を表示できない場合は、UserCheckアクションを選択します:

フォールバックアクション	動作
Allow	Webサイトやアプリケーションにアクセスできるようにします。 UserCheckクライアント(インストールされている場合)が通知を表示します。
Drop	セキュリティゲートウェイは、通知の原因となったアプリケーションに通知を表示しようとします。 それができず、UserCheck Clientがインストールされている場合、UserCheck Clientは通知を表示します。 ユーザが通知を見ない場合でも、Webサイトまたはアプリケーションをブロックします。

c. **Conditions**セクションで:

注 - このセクションは、**Ask**および**Inform**タイプのUserCheck Interactionオブジェクトにのみ表示されます。

ユーザがセキュリティゲートウェイを通じてデータを送信するために満たす必要のある条件を選択します:

条件	動作
User accepted and selected the confirm checkbox	これは、**Message**ページの**Insert User Input**メニューから**Confirm Checkbox**エレメントを挿入した場合に適用されます。 メッセージの中で、ユーザはアプリケーションにアクセスする前にチェックボックスを選択する必要があります。
User filled some textual input	これは、**Message**ページの**Insert User Input**メニューから**Textual Input**エレメントを挿入した場合に適用されます。 ユーザは、アプリケーションにアクセスする前に、テキストフィールドにテキストを入力する必要があります。 例えば、ユーザがアプリケーションを使用する際に説明を入力することを要求するかもしれません。

d. **External Portal**セクションで:

UserCheck 通知を表示する代わりに、ユーザを外部ポータルにリダイレクトするか、セキュリティゲートウェイの UserCheck ポータルにリダイレクトするかを設定します。このリダイレクトに関するユーザへの通知はありません。

これは、ユーザ名やパスワードなど、ユーザから認証情報を取得する外部システムとすることができます。この情報をセキュリティゲートウェイに送します。

i. **Redirect the user to external portal**を選択します。

ii. **URL**フィールドで、必要なURLを設定します。

iii. **オプション:** URLクエリの最後にインシデントIDを追加するには**Add UserCheck Incident ID to the URL query**を選択します。

iv. **URL Template**フィールドに、外部ポータルサーバ上のXMLファイルへのパスを入力し、セキュリティゲートウェイに返送できるようにします。

注 - このフィールドは、**Ask**および**Inform**タイプのUserCheck Interactionオブジェクトにのみ表示されます。

v. **Pre-Shared Secret**フィールドに、外部ポータルサーバをセキュリティゲートウェイに認証するために必要な文字列を入力します。

注 - このフィールドは、**Ask**および**Inform**タイプのUserCheck Interactionオブジェクトにのみ表示されます。

10. クリック**OK**。
11. この UserCheck Interaction を、使用可能な各言語および使用可能な各ビューで右ペインにプレビューします:
    - **Regular View**
    - **Mobile**
    - **Agent**
    - **Email**
    - **R80.10 and Higher Gateways**
    - **Earlier Gateways**
12. アクセスコントロールポリシーをインストールします。

プレーンテキストでEメール通知を送信

すべてのメールクライアントがリッチテキストやHTML形式のメールを扱えるわけではありません。

このようなクライアントに対応するため、HTML形式だけでなく、画像なしのプレーンテキストでEメール通知を送信するようにセキュリティゲートウェイを設定できます。

どのフォーマットを表示するかは、ユーザのメールクライアントで決まります。

1. セキュリティゲートウェイ/各クラスタメンバ/Scalable Platformセキュリティグループのコマンドラインに接続します。
2. エキスパートモードにログインします。
3. 設定ファイルをバックアップします:
   - セキュリティゲートウェイ / 各クラスタメンバ上:

     ```
     cp -v $FWDIR/conf/usrchkd.conf{,_BKP}
     ```

   - スケーラブルプラットフォームセキュリティグループ:

     ```
     g_all cp -v $FWDIR/conf/usrchkd.conf{,_BKP}
     ```

4. 設定ファイルを編集します:

   ```
   vi $FWDIR/conf/usrchkd.conf
   ```

5. 該当するパラメータの値を変更します:

   元

   ```
   :send_emails_with_no_images (false)
   ```

   先

   ```
   :send_emails_with_no_images (true)
   ```

6. 変更内容をファイルに保存し、エディタを終了します。。
7. Scalable Platformセキュリティグループ上で、変更したファイルをすべてのセキュリティグループメンバーにコピーします:

   ```
   asg_cp2blades $FWDIR/conf/usrchkd.conf
   ```

8. `userchkd`プロセスを終了して、新しい設定を読み込みます:

- セキュリティゲートウェイ / 各クラスタメンバ上：

```
killall userchkd
```

- スケーラブルプラットフォームセキュリティグループ：

```
g_all killall userchkd
```

セキュリティゲートウェイ / クラスタメンバ / セキュリティグループは、このプロセスを自動的に再起動します。

UserCheck ポータルのローカライズとカスタマイズ

詳細は、sk83700を参照してください。

外部ネットワークフィード

ネットワークフィードオブジェクトは、外部のHTTP/HTTPSサーバで生成されたフィードを強制するためのネットワークオブジェクトです。フィードには、IPアドレス(単一または範囲)、ドメイン、またはその両方を含めることができます。

例:

- シングルIP (1.1.1.1)
- 範囲 (1.1.1.1-2.2.2.2)
- IP + masklen (1.1.1.1/24)
- FQDNドメイン(google.com)
- 非FQDNドメイン(*.google.com)

フィードは、サポートされているフォーマットである必要があります(下記参照) 。セキュリティゲートウェイは、外部ソースサーバ上のフィードの変更に応じて、ネットワークフィードオブジェクトを自動的に取得、解析、更新します。アップデートを有効にするために、ポリシーをインストールする必要はありません。アクセスコントロール / HTTPS 検査 / NAT ポリシーの外部ネットワーク フィード オブジェクトをソースまたは宛先として使用できます。

注 - セキュリティゲートウェイ上でホストされているローカルフィードはサポートされていません。

使用事例

この機能は、ネットワークデータプロバイダとして外部ソースを使用し、このデータをルールベースで使用したいすべてのお客様に関連します。

ネットワークフィードを使用すると、セキュリティゲートウェイは自動的にフィードを更新します:

- フィードの手動メンテナンスを軽減
- ポリシーのインストール数を削減
- ポリシー設定の簡素化

注:

- うまく動作させるには、セキュリティゲートウェイがHTTP/HTTPS経由でフィードサーバにアクセスできる必要があります。そうでないと、セキュリティゲートウェイはフィードを取得できません。
- セキュリティゲートウェイは、最大500のネットワークフィードオブジェクトをサポートしています。各オブジェクトは最大50,000個のIPアドレスを保持できます。オブジェクトごとのドメイン数は無制限です。
- セキュリティゲートウェイは、以下のタイプのオブジェクトを合計5,000個サポートします:動的オブジェクト、更新可能オブジェクト、汎用データセンターオブジェクト、ネットワークフィードオブジェクト。セキュリティゲートウェイは、これらすべてのオブジェクトタイプを合わせて、合計350,000のIPアドレスと12,500のドメインをサポートします。
- サポートされているフィード形式:フラットリスト、JSON
- ダイナミックオブジェクトとドメインオブジェクトは、セキュリティゲートウェイのネットワークフィードを強制します。
- SmartConsoleは、フィードの更新イベント(更新中にエラー/警告が発生した場合)、およびフィードの更新に成功した場合のログを表示します。ログの検索フィールドでネットワークフィード名を検索します。
- マルチドメインサーバ環境では、グローバルオブジェクトとしてネットワークフィードを定義できます。
- セキュリティゲートウェイが常にネットワークフィードに到達できるようにします。ネットワークフィードに到達できなかったり、アクセスできなかったりした場合は、キャッシュされた最新バージョンが使用されます。
- ネットワークフィードに有効なエントリだけが含まれていることを確認してください。セキュリティゲートウェイは無効なエントリを無視し、残りのリストを使用します。

外部ネットワークフィードを設定するには

1. SmartConsoleで、オブジェクトエクスプローラに移動します。
2. **New** >**More** >**Network Object** >**Network Feed** をクリックします。

   New Network Feedウィンドウが開きます。
3. **Network**を設定:

   Feed URL- 外部サーバのフィードにアクセスするためのURLを設定します。

   ベストプラクティス - HTTPではなくHTTPSを使用します。

4. **Feed Parsing**:

   Format- フィードのコンテンツ構造を設定し、セキュリティゲートウェイでフィードを解析できるようにします。サポートされているフォーマットは、フラットリストとJSONです。

   フラットリスト形式を選択した場合は、以下を設定します:

- **Data type**- ドロップダウンメニューからドメイン、IPアドレス、またはIPアドレス/ドメインを選択し、セキュリティゲートウェイが強制するデータタイプを認識します。
- **Delimiter**- フィード内のデータ値を区切ります。
- **Ignore lines with prefix**- フィードで無視する行を定義します。

JSON形式を選択した場合は、以下を設定します:

- **Data Type**- ドロップダウンメニューからドメイン、IPアドレス、またはIPアドレス/ドメインを選択し、セキュリティゲートウェイが強制するデータタイプを認識します。
- **JSON Query**- フィードからデータを抽出する方法をJQ構文で定義。JQについての詳細は以下を参照:http://stedolan.github.io/jq/

5. **Advanced Settings**:
   - **Authentication**- URLの認証に使用するユーザ名とパスワードを入力します。
   - **Network**:
     - **Use gateway proxy for connection**- セキュリティゲートウェイが外部サーバに接続するときにプロキシを使用する場合は、このチェックボックスを選択します。
     - **Check feed interval**- セキュリティゲートウェイのフィード更新間隔(分)。デフォルトは60分です。
6. **Test Feed**:
   a. **Test Feed**ボタンをクリックして、セキュリティゲートウェイがFeed URLに接続でき、Feed URLを含むサーバーの証明書が有効であることを確認します。

      Test Feedウィンドウが開きます。

   b. **Select gateway**フィールドのドロップダウンメニューから、テストを実行するセキュリティゲートウェイを選択します:
      - テストが成功すれば、**test completed successfully**メッセージが表示されます。
      - テストに失敗すると、エラーメッセージが表示されます。
      - 無効な証明書が原因でテストに失敗した場合、以下のエラーメッセージが表示されます:**Test failed to authenticate the server certificate** 。

        この場合、信頼できるサーバであれば、エラーメッセージを無視して接続できます。

        サーバに接続するには**Accept certificate anyway**を選択します。
7. クリック**OK**。
8. アクセスコントロールルールベースで**New Network Feed**オブジェクトを使用します。
9. アクセスコントロールポリシーをインストールします。

モニタリング

セキュリティゲートウェイのネットワークフィードをモニタするには、エキスパートモードで以下のコマンドを実行します:

注 - クラスタでは、すべてのクラスタメンバでこれらのコマンドを実行してください。

操作	コマンド
ネットワークフィード更新イベントのエラーと警告メッセージを見る	`grep -i <Name of Network Feed> $FWDIR/log/efo_error.elg`
ポリシーで使用されるすべてのネットワークフィードのIPアドレスのリストを取得する	`dynamic_objects -efo_show`
特定のネットワークフィードに関連するドメインとIP範囲のリストを取得する	`dynamic_objects -efo <Name of Network Feed>`
特定のIPアドレスに関連するドメインのリストを取得する	`domains_tool -ip <IP Address>`
特定のドメインに関連するIPアドレスのリストを取得する	`domains_tool -d <Name of Domain>`

トラブルシューティング

セキュリティゲートウェイのネットワークフィードをデバッグするには、エキスパートモードで以下のコマンドを実行します:

注 - クラスタでは、すべてのクラスタメンバでこれらの手順を実行してください。

操作	手順

ネットワークフィードマッチングのためのカーネルデバッグの収集	**重要** - このカーネルデバッグは高いCPU負荷を引き起こします。メンテナンスウィンドウをスケジュールします。
	詳細は次を参照: *R82 Quantum Security Gateway Guide* > *カーネルデバッグの章*。
	1. カーネルデバッグオプションを設定:
	`fw ctl debug 0`
	`fw ctl debug -buf 8200`
	`fw ctl debug -m RAD_KERNEL all`
	`fw ctl debug -m DOMO all`
	`fw ctl debug -m UP all`
	2. カーネルデバッグの設定を調べます:
	`fw ctl debug -m`
	3. カーネルデバッグを開始します:
	`fw ctl kdebug -T -f > /var/log/kernel_debug.txt`
	4. 問題を再現します。
	5. カーネルデバッグを停止 - CTRL+Cキーを押します。
	6. カーネルデバッグオプションをリセットします:
	`fw ctl debug 0`
	7. カーネルデバッグ出力ファイルを分析します:
	`/var/log/kernel_debug.txt`

操作	手順

ポリシーインストールデバッグを収集し、ネットワークフィードに関する情報を確認します。	1. 最初のシェルでデバッグを開始します:
	`fw -d fetchlocal -d $FWDIR/state/__tmp/FW1/ >> /var/log/policy_installation.txt 2>&1`
	2. 2番目のシェルで、出力ファイルをモニタします:
	`tail -f /var/log/policy_installation.txt`
	3. 最初のシェルでデバッグを停止します:
	CTRL+Cキーを押します。
	4. 2番目のシェルで出力ファイルのモニタを停止します:
	CTRL+Cキーを押します。
	5. デバッグ出力ファイルを分析します:
	`/var/log/policy_installation.txt`

ネットワークフィードの更新イベントのデバッグを収集する	1. 最初のシェルでデバッグを開始します:
	`TDERROR_ALL_ALL=1 dynamic_objects -efo_update <Name of Network Feed> >> /var/log/network_feed_update.txt 2>&1`
	2. 2番目のシェルで、出力ファイルをモニタします:
	`tail -f /var/log/network_feed_update.txt`
	3. 最初のシェルでデバッグを停止します:
	CTRL+Cキーを押します。
	4. 2番目のシェルで、出力ファイルのモニタを停止します:
	CTRL+Cキーを押します。
	5. デバッグ出力ファイルを分析します:
	`/var/log/network_feed_update.txt`

オンプレミスのSecurity Management Serverとセキュリティゲートウェイを Infinity Portalに接続する

オンプレミスのSecurity Management Serverとセキュリティゲートウェイから Infinity Portalに接続できます。以下が可能になります:

- Infinity Portalで管理されているサービスを、Security Management Serverとセキュリティゲートウェイで実行します。

  サービスの全リストを見るには、SmartConsole > **Infinity Services**ビューにアクセスします。

  管理サーバの一部のサービスでは、構成共有とログ共有を有効にする必要があります。特定のサービスのドキュメントを参照してください。*Infinity Portal Administration Guide*。

- クラウドとオンプレミスのすべてのCheck Point製品のログを統合して表示できます。

  これにより、すべてのCheck Point製品のログやイベントを同じ場所で検索できます。

- オンプレミス管理サーバの新しい管理者機能を使用します。

  例えば、Infinity Portalを通じて、オンプレミスの管理サーバの管理APIを世界中のどこからでも安全に実行できます。

事前準備

- 使用するInfinity Portalアプリケーションまたはサービスごとに有効なライセンスが必要です。
- SmartConsole Access Controlルールベースに、Check Point セキュリティゲートウェイ用のこのルールを追加します。Check Pointサービスを更新可能なオブジェクトとして使用します(*更新可能なオブジェクト (295ページ)*):

発信元	宛先	サービス	アクション
Any	Check Pointサービス	http	許可

- Check Point以外のゲートウェイでは、sk179105のシナリオ3に記載されているドメインへのアクセスを許可します。
- 権限プロファイルで**Manage integration with Infinity Services**オプションを選択している必要があります。このオプションを選択するには

  1. **Manage & Settings** > **Permissions & Administrators** > **Permission Profiles** にアクセスします。

2. 該当するPermission Profileを開きます。
3. Managementにアクセスし、Manage integration with Infinity Servicesを選択します。

SmartConsole から Infinity Portalに Security Management Server および セキュリティゲートウェイ オブジェクトを接続するには、次の手順に従います。

1. SmartConsoleで、Infinity Servicesビューに移動します。

   Get Startedをクリックします。

   Instructionsウィンドウが開きます。

2. Infinity Portal にまだアカウントをお持ちでない場合は、Create Accountをクリックします。Infinity Portal アカウントの開設方法については、Getting Started with the Infinity Portal in the Infinity Portal Administration Guideを参照してください。
3. Connect to the Infinity Portal and get a tokenで、Get Tokenをクリックしてクラウドからトークンを取得し、Quantum Management ServerとInfinity Portalアカウント間の信頼関係を構築します。
4. 複数のアカウントを持っている場合は、Infinity Portal のSelect Accountウィンドウが開きます。

   ドロップダウンリストから該当するアカウントを選択し、Nextをクリックします。

   注 - 各管理サーバは1つのアカウントにのみ接続できます。

5. Connect my Quantum Management to Infinityページが開きます。

   Infinity Portal と管理サーバのデータを共有管理することに同意するチェックボックスを選択し、Nextをクリックします。

   Copy This to SmartConsoleページが開きます。

6. トークンをコピーし、SmartConsoleのInstructionsウィンドウに貼り付けます。

   管理サーバがInfinity Portalに接続します。

7. サービスによっては、セキュリティゲートウェイ上で実行中のエージェントが必要です。管理サーバをクラウドに接続する際に、セキュリティゲートウェイの自動オンボーディングを設定できます。Connection timing for Security Gatewaysで、いずれかのオプションを選択します。

   - Immediately(デフォルトオプション) - Security Management Server/Domain Management ServerがInfinity Portalに接続されると、サポートされているすべてのセキュリティゲートウェイが直ちに Infinity Portal に接続されます。

- **After policy installation**- サポートされているすべてのセキュリティゲートウェイは、Security Management Server/Domain Management ServerがInfinity Portalに接続され、アクセスコントロールポリシーがインストールされた後にのみ、Infinity Portalに接続されます。

8. **Connect**をクリックします。

オンプレミスの管理サーバの構成情報をInfinity Portalと共有するには

1. SmartConsole >**Infinity Services**ビューで、ページ下部の**Infinity Portal Settings** >**Configuration Sharing**を開きます。
2. **Edit**をクリックします。

   Configuration Sharingウィンドウが開きます。
3. **Enable**ボタンを**ON**に合わせ、**OK**をクリックします。

管理サーバの設定情報がInfinity Portalと同期されます。

注- Infinityポータルでは、管理サーバから共有されたオブジェクトを編集できません。

オンプレミスの管理サーバのログ情報をInfinity Portalで共有するには

1. SmartConsole > **Infinity Services**ビュー >**Infinity Portal Settings** (ページの一番下) > **Log Sharing**に移動します。
2. **Edit**をクリックします。

   Log Sharingウィンドウが開きます。
3. ログ情報を共有したい製品を選択します:
   - **All products**
   - **Specific products**-ドロップダウンリストから該当する製品を選択します。
4. **Enable**ボタンを**ON**に変更し、**OK**をクリックします。

管理サーバは、ログ情報をInfinity Portalと同期するようになりました。

注 - スタンドアロンでログ共有を有効にするには、サーバに以下の環境が必要です:

- 1秒あたりのログ受信数が500件未満の場合、少なくとも2つのCPUコアと16GBのRAMが必要です。
- 1秒間に500件以上のログを受信する場合、少なくとも4つのCPUコアと16GBのRAMが必要です。

Infinity Portalへのセキュリティゲートウェイの接続タイミングを設定するには

1. SmartConsole > **Infinity Services**ビューで、ページ下部の**Gateways Connector**にアクセスします。
2. 設定を変更するには、**Edit**をクリックします。
3. この2つのオプションから1つを選択します:
   - **Immediately**(デフォルトオプション) - Security Management Server/Domain Management ServerがInfinity Portalに接続されると、サポートされているすべてのセキュリティゲートウェイが直ちにInfinity Portalに接続されます。
   - **After policy installation**- サポートされているすべてのセキュリティゲートウェイは、Security Management Server/Domain Management ServerがInfinity Portalに接続され、アクセスコントロールポリシーがインストールされた後にのみ、Infinity Portalに接続されます。

   注 - セキュリティゲートウェイのオンボーディングの詳細については、sk180557を参照。

SmartConsoleからInfinity Portalの該当サービスに接続するには

1. 左側のナビゲーションパネルで**Infinity Services**をクリックします。
2. 該当するサービスに行き、接続します。

各サービスの詳細については*Infinity Portal Administration Guide*。

トラブルシューティング

トラブルシューティングの問題については、sk181504を参照してください。

HTTPSインスペクション

HTTPSインターネットトラフィックは、TLS(トランスポートレイヤーセキュリティ) プロトコルを使用し、データのプライバシーと完全性を与えるために暗号化されます。しかし、HTTPSトラフィックにはセキュリティリスクがあり、違法なユーザアクティビティや悪意のあるトラフィックを隠してしまう可能性があります。セキュリティゲートウェイの有効なSoftware Bladesでは、HTTPSトラフィックは暗号化されているため検査できません。HTTPSインスペクションにより、セキュリティゲートウェイはTLS接続を傍受し、有効なSoftware Bladesによる検査のためにトラフィックを復号します。

HTTPSインスペクションには2つのモードがあります:

- **Outbound HTTPS Inspection**- 内部クライアントから外部サイトまたはサーバに送信される悪意のあるトラフィックから保護する。
- **Inbound HTTPS Inspection**- インターネットや外部ネットワークから届く悪意のあるリクエストから内部サーバを保護する。

セキュリティゲートウェイは証明書を使用し、クライアントコンピュータと安全なWebサイトとの仲介役となります。すべてのデータはHTTPSインスペクションのログで非公開にされます。HTTPSインスペクション権限を持つ管理者だけが、このようなログのすべてのフィールドを見ることができます。

R80.20以降のHTTPSインスペクションの新機能については、sk163594を参照してください。

HTTPS接続の遮断

アウトバウンド HTTPSインスペクション

アウトバウンド接続は、内部クライアントから外部サーバに届くHTTPS接続です。

アウトバウンド接続フロー

1. HTTPSリクエスト(内部クライアントから外部サーバへ) がセキュリティゲートウェイに到着します。
2. セキュリティゲートウェイはHTTPSリクエストをインターセプトします。
3. セキュリティゲートウェイは、HTTPSリクエストが既存のHTTPSインスペクションルールに一致するかどうかを判断します。
   - HTTPSリクエストがルールに一致**しない**場合、セキュリティゲートウェイはHTTPS接続をインターセプトしません。

     この場合、HTTPSインスペクションはバイパスされます。
   - HTTPSリクエストがルールに一致する場合、セキュリティゲートウェイはHTTPS 接続をインターセプトし、次のステップに進みます。
4. セキュリティゲートウェイは外部サーバの証明書を検証します。

   デフォルトでは、セキュリティゲートウェイは証明書の失効を確認するためにオンライン証明書ステータスプロトコル(OCSP) を使用します。

   証明書がOCSPをサポートしていない場合、セキュリティゲートウェイは証明書失効リスト(CRL) を使用して証明書の失効を確認します。
5. セキュリティゲートウェイは、外部サーバとの接続のために新しい証明書を作成します。
6. セキュリティゲートウェイはHTTPSトラフィックを復号します。
7. セキュリティゲートウェイは、有効化されたSoftware Bladesを呼び出して、復号されたHTTPSトラフィックを検査します。
8. セキュリティポリシーがこのトラフィックを許可している場合、セキュリティゲートウェイはHTTP接続を暗号化します。
9. セキュリティゲートウェイは外部サーバにHTTPSリクエストを送信します。

インバウンド HTTPSインスペクション

インバウンド接続は、外部クライアントから到着し、DMZまたは内部ネットワーク内のサーバに接続するHTTPS接続です。

インバウンド接続フロー

1. HTTPSリクエスト(外部クライアントから内部サーバへ)がセキュリティゲートウェイに到着します。

   注 - セキュリティゲートウェイ/クラスタは、自分に向けられているトラフィックに対してHTTPSインスペクションを実行しないように意図的に設計されています。この動作を変更するには、sk114574に従います。

2. セキュリティゲートウェイでHTTPSリクエストがインターセプトされます。
3. セキュリティゲートウェイは、HTTPSリクエストが既存のHTTPSインスペクションルールに一致するかどうかを判断します。
   - HTTPSリクエストがルールに一致**しない**場合、セキュリティゲートウェイはHTTPS接続をインターセプトしません。

     この場合、HTTPSインスペクションはバイパスされます。
   - HTTPSリクエストがルールに一致する場合、セキュリティゲートウェイはHTTPS接続をインターセプトし、次のステップに進みます。
4. セキュリティゲートウェイは、内部サーバの証明書を使用して、外部クライアントとのHTTPS接続を作成します。
5. セキュリティゲートウェイは内部サーバとのHTTPS接続を新規に作成します。
6. セキュリティゲートウェイはHTTPSトラフィックを復号します。
7. セキュリティゲートウェイは、有効化されたSoftware Bladesを呼び出して、復号されたHTTPSトラフィックを検査します。
8. セキュリティポリシーがこのトラフィックを許可している場合、セキュリティゲートウェイはHTTP接続を暗号化します。
9. セキュリティゲートウェイは内部サーバにHTTPSリクエストを送信します。

HTTPSインスペクションの開始

このセクションでは、アウトバウンドとインバウンドのHTTPSトラフィックをインターセプトするために、セキュリティゲートウェイを設定する方法の例を示します。

ステップ	手順
1	セキュリティゲートウェイの該当するSoftware Bladesを有効にします。 復号されたHTTPSトラフィックを検査するには、有効なSoftware Bladesのセキュリティゲートウェイで HTTPSインスペクションを有効にする必要があります。
2	該当するHTTPSインスペクションポリシー(インバウンドおよびアウトバウンド) を設定します。 参照: *HTTPSインスペクションポリシー (545ページ)*
3	インバウンド証明書を使用するようにセキュリティゲートウェイを設定します。 参照: *インバウンドCA証明書の操作 (549ページ)*。
4	セキュリティゲートウェイでHTTPSインスペクションを設定します: a. セキュリティゲートウェイが送信証明書を使用するように構成し、組織内に証明書を配置します。 参照: *アウトバウンド CA 証明書の操作 (554ページ)* b. セキュリティゲートウェイでHTTPSインスペクションを有効にします。 c. 追加設定を行います。 参照: *セキュリティゲートウェイでのHTTPSインスペクションの設定 (550ページ)*。
5	アクセスコントロールポリシーをインストールします。

HTTPSインスペクションポリシー

HTTPSインスペクションルールは、セキュリティゲートウェイがHTTPS接続をどのように遮断するかを定義します。

R82以降、HTTPSインスペクションポリシーは「インバウンドポリシー」と「アウトバウンドポリシー」に分かれています。

HTTPSインスペクションルールは、URLフィルタリングカテゴリを使用して、異なるWebサイトやアプリケーションのトラフィックを識別することができます。例えば、ユーザのプライバシーを保護するために、銀行や金融機関へのHTTPSトラフィックを無視するルールを使用することができます。

デフォルトでは、セキュリティゲートウェイは、有効化されたすべてのサポート対象Software Bladesに対してHTTPSインスペクションを実施します。

HTTPSインスペクションに対応したSoftware Bladesは次のとおりです。

- アクセスコントロール:
  - アプリケーション コントロール
  - URL フィルタリング
  - コンテンツアウェアネス
  - DLP (データ損失防止)
- 脅威対策:
  - IPS
  - アンチウイルス
  - アンチボット
  - Threat Emulation
  - Threat Extraction
  - ゼロフィッシング

特定のSoftware BladesにHTTPSインスペクションを適用するには、以下の手順を実行する必要があります:

1. セキュリティゲートウェイオブジェクトで必要なSoftware Bladeを有効にします。
2. HTTPSインスペクションポリシーで適用可能なルールを作成し、**Blade** カラムで必要なSoftware Bladeを選択します。

異なるポリシーパッケージで異なるHTTPSインスペクションレイヤーを作成できます。新しいポリシーパッケージを作成する場合、あらかじめ定義されたHTTPSインスペクションレイヤを使用するか、セキュリティニーズに合わせてHTTPSインスペクションレイヤをカスタマイズすることができます。

HTTPSインスペクションレイヤは、複数のポリシーパッケージで共有することができます。

HTTPSインスペクションセキュリティポリシーのカラム

HTTPSインスペクションセキュリティポリシールールのカラムです:

(カラムを表示または非表示にするには、任意のカラムのヘッダを右クリックします)。

カラム	説明
No.	HTTPSインスペクションルールベースのルール番号。
Name	システム管理者がこのルールに付ける名前。
Source	トラフィックの開始位置を定義するネットワークオブジェクト。
Destination	トラフィックの宛先を定義するネットワークオブジェクト。
Services	傍受または迂回されるサービス(プロトコル)。 デフォルトでは、ポート443の`https`、ポート8080の`HTTP_and_HTTPS proxy`。 このカラムでサービスの追加や削除ができます。
Site Category	傍受または迂回されたアプリケーションやWebサイトのカテゴリ。
Action	セキュリティゲートウェイがHTTPSトラフィックをルールにマッチさせたときに実行するアクション。 ■ **Inspect**- セキュリティゲートウェイはHTTPS接続を傍受する。 ■ **Bypass**- セキュリティゲートウェイはHTTPS接続を傍受しない。 **重要** - 接続フローとこのアクションの詳細については、以下を参照してください: ■ *アウトバウンドHTTPSインスペクション (542ページ)* ■ *インバウンドHTTPSインスペクション (543ページ)*
Track	トラフィックがルールに一致したときに行われるアクションを追跡し、ログに記録します。
Blade	デフォルトでは、「**All**」という値が設定され、有効化されたすべてのSoftware Bladesで復号されたHTTPSトラフィックが検査されます。 特定のSoftware Bladeを選択して、復号されたHTTPSトラフィックを検査することができます。

カラム	説明
Install On	このHTTPSインスペクションポリシーを実施するセキュリティゲートウェイ。 デフォルトでは、このカラムにはオブジェクト **Policy HTTPS Targets** 。 このオブジェクトは、HTTPSインスペクションが有効になっているすべてのセキュリティゲートウェイに自動的に適用されます。 このカラムでは、HTTPSインスペクションが有効になっているセキュリティゲートウェイのみを選択できます。
Certificate	このカラムは "Inbound Policy "にのみ存在します。 このカラムでは、内部サーバがルールに使用する証明書を選択します。
Comment	ルールの説明を追加するオプションのフィールド。

HTTPSインスペクションポリシーの設定

対応するアウトバウンドとインバウンドのポリシー内で、アウトバウンドとインバウンドのトラフィックに対して個別のHTTPSインスペクションルールを確立します。

インバウンドルールでは、内部サーバごとに異なる証明書を使用します。

また、機密性が高く、傍受されるべきではないトラフィック用にバイパスルールを作成することもできます。バイパスルールがOutbound Policyの一番上にあることを確認してください。

重要 - 送信ポリシーまたは受信ポリシーを変更するには、アクセスコントロールポリシーをインストールする必要があります。

アウトバウンドHTTPSインスペクションルールベースのサンプル

この表は、典型的なポリシーのHTTPSインスペクションアウトバウンドルールベースのサンプルを示しています。

いいえ	名前	発信元	宛先	サービス	サイトカテゴリ	アクション	追跡	インストール先
1	金融関連サイト	*Any	Internet	https HTTP_ HTTPS_ proxy	Financial Services	Bypass	Log	HTTPS Policy Targets
2	アウトバウンドトラフィック	*Any	Internet	https HTTP_ HTTPS_ proxy	Any	Inspect	Log	HTTPS Policy Targets

1. **Financial sites**- これは、「Financial Services」カテゴリに定義されているWebサイトへのHTTPS接続を遮断しないバイパスルールです。
2. **Outbound traffic**- このルールは、インターネットへのHTTPS接続を遮断します。このルールでは、アウトバウンドCA証明書を使用します。

インバウンドHTTPSインスペクションルールのサンプル

この表は、典型的なポリシーのHTTPSインスペクションインバウンドルールのサンプルを示しています。

いいえ	名前	発信元	宛先	サービス	アクション	証明書
1	インバウンドトラフィック	*Any	WebCalendarServer	https	Inspect	WebCalendarServer CA

Inbound traffic- このルールは、ネットワークオブジェクトWebCalendarServerへのHTTPS接続を遮断します。このルールではWebCalendarServer証明書を使用します。

HTTPSインスペクションポリシーの実施

HTTPSインスペクションルールベースは2つのステップで実施されます:

1. 接続をルールベースと照合します。
2. 実行するアクションを計算します。

アクションは、マッチしたルール、マッチしたルールに定義されたSoftware Blades、およびルールの例外に従って計算されます。特定のシナリオでは、マッチしたルールのアクションは**Inspect**ですが、ステップ2の結果、アクションは**Bypass**に変更されます。このような場合、一致したルールのデータとともにHTTPSインスペクションログが送信されるが、ログに記録されるアクションは**Bypass**です。

インバウンドCA証明書の操作

設計上、セキュリティゲートウェイ / Security クラスタは、意図的にHTTPS Inspection を実行しないように設定されています。この動作を変更するには、sk114574に従います。

インバウンドHTTPSインスペクションのサーバ証明書の割り当て

組織外のクライアントが内部のWebサーバ(たとえば、セキュリティゲートウェイの背後にある組織のDMZにあるサーバ) にHTTPS接続を開始すると、セキュリティゲートウェイはそのトラフィックを傍受することができます。

このシナリオでHTTPSインスペクションを実行するには、セキュリティゲートウェイが内部Webサーバになりすます必要があります。

このためには、セキュリティゲートウェイが内部WebサーバのTLS証明書を提示し、サーバの証明書秘密鍵にアクセスできる必要があります。

したがって、管理者は、証明書と秘密鍵を内部Webサーバから*.p12フォーマット(両方を含む) でエクスポートし、このP12ファイルをSmartConsoleにインポートすることが重要です。

サーバの証明書をインポートした後、管理者は対応する証明書オブジェクトをHTTPSインスペクション受信ポリシーに追加できます。

インバウンドHTTPSインスペクション用のサーバ証明書を追加するには

ステップ	手順
1	SmartConsoleで、**Security Policies**ビュー >**HTTPS Inspection** >**Inbound Policy** > 上のツールバーから、**Inbound Certificates**をクリックします。
2	**Import**をクリックします。 **Import Inbound Certificate**ウィンドウが開きます。
3	**Certificate name**と**Comment**を入力します(任意) 。

ステップ	手順
4	証明書ファイルを参照します。
5	**Password**を入力します。 サーバで証明書の秘密キーを保護するために使用したものと同じパスワードを入力します。
6	クリック**OK**。
7	**Close**をクリックします。

サーバ証明書を初めてインポートするときは、**Successful Import**ウィンドウが表示されます。
HTTPSインスペクションポリシーでオブジェクトを追加する場所を示しています。

サーバ証明書をインポートするたびにウィンドウを表示したくない場合は、**Don't show this again**をクリックして**Close**をクリックします。

セキュリティゲートウェイでのHTTPSインスペクションの設定

各セキュリティゲートウェイで個別にHTTPSインスペクションを設定する必要があります。

セキュリティゲートウェイでHTTPSインスペクションを設定するには

ステップ	手順
1	SmartConsole ゲートウェイ & サーバビューで、セキュリティゲートウェイオブジェクトをダブルクリックします。
2	HTTPSインスペクションをクリックします。
3	オプション: 送信CA証明書がすでに別のセキュリティゲートウェイ用に作成またはインポートされている場合は、グローバル証明書を使用するか、各セキュリティゲートウェイ用に特定の証明書を選択して上書きすることができます。 グローバル証明書を上書きするには、セキュリティゲートウェイオブジェクトの**HTTPS Inspection** >**Step 1** に移動し、**Override global setting** を選択して、ドロップダウンリストから必要な証明書を選択します。
4	**Import or Create an outbound CA certificate for HTTPS Inspection**。 参照: *アウトバウンド CA 証明書の操作 (554ページ)*。

ステップ	手順
5	**Export and Deploy the outbound certificate in your organization**。 参照: *生成されたCA証明書のエクスポートと配置 (557ページ)*。
6	**Step 3**で、**Enable HTTPS Inspection**を選択します。
7	HTTPSインスペクションの設定**Deployment Mode**： ■ **Full inspection**- HTTPS接続は、HTTPSインスペクションポリシーに基づいて遮断されます。 ■ **Learning mode**- HTTPSインスペクションの部分的なデプロイメントを構成して、接続性とパフォーマンスの問題への影響を見積もることができます。**Learning mode**では、セキュリティゲートウェイはトラフィックのごく一部を傍受し、接続性の問題を特定し、設定されたHTTPSインスペクションポリシーで予想されるリソース消費量を推定します。 学習モードの効果またはすべてのセキュリティゲートウェイのステータスを表示するには、セキュリティポリシービュー > HTTPSインスペクション >**Outbound Policy**または**Inbound Policy** > **HTTPS Inspection Tools**セクションで**Deployment**をクリックします。 詳細: *HTTPSインスペクションのデプロイメント図 (553ページ)*。

ステップ	手順
8	**Additional Settings** > **Edit** で、クライアント側とサーバ側のフェイルモードを設定します。 クライアントまたはサーバの接続エラーの場合、これらのモードのいずれかを選択できます: ■ **フェイルオープン** - セキュリティゲートウェイは、サーバ側またはクライアント側で失敗した接続に対してHTTPSインスペクションを実行しません(HTTPSインスペクションはバイパスされます) 。 ■ **フェイルクローズ** - セキュリティゲートウェイは、内部システムエラーまたはサーバ接続エラー(サーバ側エラー) 、またはクライアント接続の問題の結果として失敗した接続をブロックします。 グローバル設定に基づいてサーバとクライアントのエラーを処理することも、特定のセキュリティゲートウェイ用にグローバル設定を上書きすることもできます。すべてのセキュリティゲートウェイにフェイルモード設定をグローバルに設定するには、以下を参照してください。*Fail Mode (562ページ)*。 **特定のセキュリティゲートウェイにフェイルモードを設定するには** a. **Additional Settings**で、**Edit**をクリックします。 **HTTPS Inspection Settings**ウィンドウが開きます。 b. **Server Side Fail Mode**の設定 - 内部システムエラーまたはサーバ接続エラーの場合、これらのオプションのいずれかを選択します: ■ **Use the global setting**- デフォルトのグローバル設定は**Fail Open**です。 ■ **Override global settings**- **Fail-Open**または**Fail-Close**を選択します。 c. **Client-Side Fail Mode**- クライアント接続の問題が検出された場合は、以下の2つのオプションのいずれかを選択します: ■ **Use the global setting**- デフォルトのグローバル設定は**Fail Open**です。 ■ **Override global settings**- **Fail-Open**または**Fail-Close**を選択します。 **注:** ■ **Fail-Open**モードでは、セキュリティゲートウェイは最初の接続をブロックするが、同じ送信元と宛先ホスト名を持つ後続の接続は遮断せず、バイパスします。 ■ セキュリティゲートウェイのバージョンR81.20以下では、クライアント側でエラーが発生した場合、常に接続がブロックされます(**Fail-Close**) 。これらのバージョンでは動作変更はできません。

ステップ	手順
9	**Bypass Under Load**の設定 - この機能は、セキュリティゲートウェイに高負荷が発生した場合に接続を許可します(HTTPSインスペクションとは限らない)。セキュリティゲートウェイは、接続の中断を避けるため、CPUスパイクに素早く反応し、負荷が安定するまで一時的にHTTPSインスペクションをバイパスします。バイパスの間、セキュリティゲートウェイはHTTPSトラフィックを傍受しません。セキュリティゲートウェイが安定した後、バイパス時間を最小化するためにHTTPSインスペクションの再開を試みます。インスペクション再開後に持続的な高負荷が検出された場合、セキュリティゲートウェイは安定性を維持するためにバイパス時間を徐々に長くします。 この機能はデフォルトでは**無効**になっています。 **重要** -「Bypass Under Load」のログタイプを設定するには、**Security Policies** > HTTPSインスペクション >**Inbound Policy** または**Outbound Policy** >**HTTPS Inspection Tools** >**Advanced Settings** >**Other** >**Bypass Under Load Logging** にアクセスします。 **注** - セキュリティゲートウェイごとに**Bypass Under Load**を個別に設定します。この機能のグローバル設定はありません。
10	クリック**OK**、アクセスコントロールポリシーをインストールします。

HTTPSインスペクションのデプロイメント図

このビューでは、学習モードでHTTPSインスペクションが有効になっているセキュリティゲートウェイのステータスと推奨事項が表示されます。

また、各セキュリティゲートウェイのインスペクション状況も次のように表示されます:

- **Full inspection**- セキュリティゲートウェイでフルインスペクションが設定されている場合に表示されます。セキュリティゲートウェイは、設定されたHTTPSインスペクションポリシーに基づいて、すべてのHTTPS接続を遮断します。
- **Learning mode**- セキュリティゲートウェイで学習モードが設定されている場合に表示されます。ここでは、学習モード導入の効果と、HTTPSインスペクションのデプロイメントに関する推奨事項を確認できます。
- **Categorized HTTPS Inspection only**- HTTPSインスペクションがセキュリティゲートウェイで無効になっており、分類されたHTTPS Webサイトがグローバルに設定されている場合に表示されます(**Manage and Settings**ビュー > **Blades** > **Application Control & URL Filtering** > **Advanced Settings** >**URL Filtering**)。
- **Disabled**- HTTPSインスペクションがセキュリティゲートウェイで有効になっておらず、HTTPS Webサイトの分類オプションが無効になっています。

アウトバウンド CA 証明書の操作

送信CA証明書は、Security Management Serverで管理されるセキュリティゲートウェイで使用されます。セキュリティゲートウェイの1つでHTTPSインスペクションを初めて有効にする場合、HTTPSインスペクションのアウトバウンドCA証明書を作成するか、組織内にすでに配布されているCA証明書をインポートする必要があります。R82以降、追加の送信証明書を作成またはインポートできます。

送信CA証明書の作成

アウトバウンドCA証明書は、ファイル拡張子CERで保存され、パスワードを使ってファイルの秘密鍵を暗号化します。セキュリティゲートウェイは、このパスワードを使用してHTTPSインスペクション用の証明書に署名します。このパスワードは、CA証明書をインポートする他のSecurity Management Serverがファイルを開く際にも使用されるため、安全に保管する必要があります。

アウトバウンドCA証明書を作成したら、それをエクスポートして内部クライアントに配布できるようにする必要があります。生成されたアウトバウンドCA証明書を内部クライアントに導入しない場合、HTTPSサイトに接続する際に、ユーザはブラウザでTLSエラーメッセージを受け取ります。このような接続をログに記録するトラブルシューティングオプションを設定することができます。

送信CA証明書を作成したら、HTTPSインスペクションポリシーで送信HTTPSトラフィックを遮断するルールに使用します。

送信CA証明書を作成するには

ステップ	手順
1	SmartConsoleの**Gateways & Servers**ビューで、セキュリティゲートウェイオブジェクトをダブルクリックします。 **ゲートウェイProperties**のウィンドウが開きます。
2	ナビゲーションツリーで、**HTTPS Inspection**をクリックします。
3	**Step 1**で、**Create**をクリックします。 **注** - 最初のアウトバウンド証明書を作成するには、**Security Policies** > HTTPSインスペクション >**Outbound Policy** > 上部ツールバーから、**Outbound Certificates**をクリックします。
4	必要な情報を入力します。 ■ **Issued by (DN)**- 組織のドメイン名を入力します。 ■ **Private key password**- CA証明書の秘密鍵の暗号化に使用するパスワードを入力します。 ■ **Retype private key password**- パスワードを再度入力します。 ■ **Valid from**- CA証明書が有効な日付範囲を選択します。

ステップ	手順
5	クリックOK。
6	CA証明書をエクスポートしてデプロイします。 参照: *生成されたCA証明書のエクスポートと配置 (557ページ)*。

アウトバウンドCA証明書のインポート

組織内にすでに配備されているCA証明書をインポートしたり、あるSecurity Management Serverで作成されたCA証明書を別のSecurity Management Serverにインポートしたりできます。

ベストプラクティス - プライベートCA証明書を使用します。

HTTPSインスペクションんが有効になっているセキュリティゲートウェイを持つ各Security Management Serverについて、以下を行う必要があります:

1. CA証明書をインポートします。
2. Security Management ServerがCA証明書ファイルを開き、ユーザの証明書に署名する際に使用するパスワードを入力します。このパスワードは、新しいSecurity Management Serverに証明書をインポートするときのみ使用します。

送信CA証明書をインポートするには

ステップ	手順
1	CA証明書が別のSecurity Management Serverで作成された場合は、その証明書が作成されたSecurity Management Serverから証明書をエクスポートします。 参照: *Security Management Serverから別のSecurity Management Serverへの証明書のエクスポート (559ページ)*。
2	SmartConsoleの**Gateways & Servers**ビューで、Security Gatewayオブジェクトをダブルクリックします。
3	ナビゲーションツリーで、**HTTPS Inspection**をクリックします。
4	**Step 1**で、**Import**をクリックします。 **注** - 最初に作成した送信証明書は、**Security policies** > HTTPSインスペクション > **Outbound Policy** > 上のツールバーから**Outbound Certificate**をクリックしてインポートすることもできます。
5	証明書ファイルを参照します。
6	**private key password**を入力します。

ステップ	手順
7	クリックOK。
8	CA証明書が別のSecurity Management Serverで作成された場合は、それをクライアントに配置します。 クリック*生成されたCA証明書のエクスポートと配置 (557ページ)*。

生成されたCA証明書のエクスポートと配置

HTTPSインスペクションが使用する生成されたCA証明書に関する警告がユーザに表示されないようにするため、HTTPSインスペクションが使用する生成されたCA証明書を信頼できるCAとしてインストールします。Windows GPOなど、さまざまな配布メカニズムでCAを配布することができます。これにより、生成されたCAがクライアントコンピュータ上の信頼できるルート証明書リポジトリに追加されます。

ユーザが標準アップデートを実行すると、生成されたCAがCAリストに表示され、ブラウザで証明書の警告が表示されなくなります。

証明書をGPOで配布するには

ステップ	手順
1	セキュリティゲートウェイから証明書をエクスポートします: 送信証明書をエクスポートするには、以下の2つのオプションのいずれかを使用します: **オプション1** a. SmartConsoleで、[Security Policies] ビュー > [HTTPS Inspection] >**Outbound Policy** を開きます。 b. 上部のツールバーで**Outbound Certificates**をクリックします。 **Manage Outbound Certificates**ウィンドウが開きます。 c. 必要な証明書を選択し、ボタンをクリックします。 d. 証明書を保存する必要なフォルダを選択し、**Save**をクリックします。 **オプション2** a. SmartConsole > [Gateways & サーバ] ビューで、必要なセキュリティゲートウェイオブジェクトをダブルクリックします。 Security Gatewayオブジェクトエディタが開きます。 b. 左のメニューからHTTPSインスペクションに移動します。 c. **Step 2**で、**Export Certificate**をクリックします。 d. 証明書を保存するフォルダを選択して**Save**
2	**グループポリシー管理コンソール**を使用して、証明書を**Trusted Root Certification Authorities**証明書ストアに追加します。 参照: *グループポリシーを使用した証明書の展開 (558ページ)*。
3	組織内のクライアントコンピュータにGPOポリシーをプッシュします。 **注** - CA証明書がクライアントコンピュータの組織単位にプッシュされていることを確認してください。

ステップ	手順
4	クライアントコンピュータの1台からHTTPSサイトにアクセスして、CA証明書の配布をテストします。 また、CA証明書に、**Issued by** フィールドに作成したCA証明書に入力した名前が表示されていることを確認します。

グループポリシーを使用した証明書の展開

この手順を使用して、Active Directoryドメインサービスとグループポリシーオブジェクト(GPO)を使用して、証明書を複数のクライアントコンピュータに展開できます。GPOは複数の設定オプションを含むことができ、GPOの適用範囲内のすべてのコンピュータに適用されます。

重要 - この手順を実行するには、ローカルの管理者グループのメンバ、または同等のメンバである必要があります。

グループポリシーを使用して証明書を配置するには

ステップ	手順
1	Microsoft Windows Serverで、**Group Policy Management Console**を開きます。
2	既存のGPOを検索するか、証明書設定を含む新しいGPOを作成します。GPOが、ポリシーの影響を受けさせたいユーザのドメイン、サイト、または組織ユニットに関連付けられていることを確認します。
3	GPOを右クリックし、**Edit**を選択します。 **Group Policy Management Editor**が開き、ポリシーオブジェクトの内容が表示されます。
4	**Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Trusted Publishers**を開きます。
5	**Action** >**Import** をクリックします。
6	**Certificate Import Wizard**にある手順で、SmartConsoleからエクスポートした証明書を探し、インポートします。
7	ナビゲーションペインで、**Trusted Root Certification Authorities**をクリックし、手順5～6を繰り返して、そのストアに証明書のコピーをインストールします。

Security Management Serverから別のSecurity Management Serverへの証明書のエクスポート

組織内で複数のSecurity Management Serverを使用している場合、他のSecurity Management Serverにインポートする前に、*最初に*CA証明書を作成したSecurity Management Serverから "`export_https_cert`" CLIコマンドでエクスポートすることが重要です。

コマンド構文

```
export_https_cert -help
```

```
export_https_cert {[-local] | [-s <server address>]} [-f
<certificate file name in the FWDIR/tmp/ directory>]
```

CA証明書をエクスポートするには

Security Management Serverで、次のコマンドを実行します。

```
$FWDIR/bin/export_https_cert -local -f <certificate file name in
the FWDIR/tmp/ directory>
```

例:

```
$FWDIR/bin/export_https_cert -local -f mycompany.cer
```

注 - Multi-Domain Security Management Serverでは、該当するDomain Management Server(`mdsenv <IP Address of Domain Management Server>`)のコンテキストでこのコマンドを実行する必要があります。

アウトバウンド HTTPS 検査における信頼できる CA との連携

クライアントがサーバーへのTLS接続を開始すると、セキュリティゲートウェイはTLS接続をインターセプトする。セキュリティゲートウェイはトラフィックをインターセプトし、セキュリティゲートウェイから指定されたサーバーへの新しいTLS接続を作成する。

セキュリティゲートウェイが指定されたサーバーにTLS接続を確立するとき、サーバー証明書を検証する必要がある。

HTTPSインスペクションには、あらかじめ設定された信頼できるCAのリストが付属しています。このリストはCheck Pointによって必要に応じて更新され、Check Pointダウンロードセンターから管理サーバに自動的にダウンロードされます。Security Management Serverでトラスト CAのアップデートを取得した後、セキュリティゲートウェイにポリシーをインストールする必要があります。自動更新オプションを無効にして、信頼済みCAリストを手動で更新することを選択できます。sk64521を参照してください。

セキュリティゲートウェイが信頼できないサーバ証明書を受け取った場合、デフォルトでは、ユーザは生成された証明書ではなく、自己署名証明書を取得します。サーバのセキュリティ証明書に問題があることをユーザにページで通知しますが、ユーザはサーバに進むことができます。

信頼できないサーバ証明書をブロックするように、デフォルトの設定を変更することができます。セキュリティポリシー > HTTPSインスペクション > HTTPSインスペクションツール >**Advanced Settings** >**Server Validations** >**Untrusted server certificates** を選択します。

信頼済み証明書のリストを管理するには、SmartConsoleで、**Security Policies** > HTTPSインスペクション > HTTPSインスペクション**Tools**セクションで、**Trusted Certificates**をクリックします。

Trusted Certificatesウィンドウで実行できます:

- **Trusted CAs Package**タブ:
  - 信頼できるCAパッケージが最新かどうかを確認できます。ダウンロードされたパッケージのバージョン、最終アップデートのタイムスタンプ、これらのステータスの最終チェックに関する詳細を確認できます。証明書を更新する方法は2つあります。
    - 自動更新:

      Update Trusted CA package automaticallyを選択します。Trusted CAパッケージは、1日1回午前2時に自動的に更新されます。
    - 手動更新:

      Updated Trusted CAs Package manuallyを選択し、**Update Now**または**Import Trusted CAs Package**をクリックしてパッケージを手動で更新します。

- **Certificates**セクションでは、パッケージに含まれるすべての証明書の表示、証明書のエクスポート、証明書の有効化または無効化を行うことができます。

  証明書を有効または無効にするには

  1. チェックボックスを使用して、該当する証明書を選択します。

     注 - 一番上のチェックボックスをクリックすると、すべての証明書を選択できます。

  2. トップメニューから、**Actions**をクリックし、**Enable**または**Disable**

- **Custom Trusted Certificates**タブでは、証明書のインポート、エクスポート、削除ができます。

注 - Trusted CA設定の変更を適用するには、該当するセキュリティゲートウェイにポリシーをインストールします。

HTTPSインスペクションのグローバル設定

セキュリティポリシー > HTTPSインスペクション > **HTTPS Inspection Tools** > **Advanced Settings** で、すべてのセキュリティゲートウェイのHTTPSインスペクショングローバル設定を構成できます。

Fail Mode

フェイルモードのグローバル設定を変更するには

1. **Security Policies**ビュー > HTTPSインスペクション > **Inbound Policy**または**Outbound Policy** > **HTTPS Inspection Tools**セクションで、**Advanced Settings**をクリックします。
2. **Fail Mode**にアクセスし、該当する設定を選択します。
   a. **Server Side Fail Mode**で、いずれかのオプションを選択します。
      - **Bypass all requests (Fail-Open)**
      - **Block all requests (Fail-Close)**
   b. **Client Side Fail Mode**で、いずれかのオプションを選択します。
      - **Bypass all requests (Fail-Open)**
      - **Block all requests (Fail-Close)**

注:
- フェイルオープンモードでは、セキュリティゲートウェイは最初の接続をブロックしますが、同じ送信元と宛先ホスト名を持つ後続の接続は遮断せず、バイパスします。
- セキュリティゲートウェイのバージョンR81.20以下では、クライアント側でエラーが発生した場合、常に接続がブロックされます(フェイルクローズ)。これらのバージョンでは動作の変更はできません。

Categorization Mode

HTTPSサイトを分類するモードを設定します:

- **Background**- 分類が完了するまで、すべてのリクエストは許可されます。リクエストがキャッシュされた応答で分類できない場合、分類されていない応答を受け取ります。サイトへのアクセスは許可されます。バックグラウンドでは、Check Point Online Web Service が分類処理を続行します。レスポンスは、将来のリクエストのためにローカルにキャッシュされます。このオプションは、分類処理の時間を短縮します。
- **Hold**- これはデフォルトの設定です。キャッシュされたレスポンスで分類できなかったリクエストは、Check Point Online Web Service による分類が完了するまでブロックされたままになります。

Server Validations

セキュリティゲートウェイがWebサイトサーバから信頼できない証明書を受信した場合、このセクションの設定により、接続を切断するタイミングが定義されます。

- **Untrusted server certificate**:
  - 信頼できないサーバ証明書を持つサイトからのトラフィックが選択されると、即座にドロップされます。ブラウザがWebページを表示できないというエラーページが表示されます。
  - クリアすると、信頼できないサーバからのトラフィックがある場合、自己署名証明書がクライアントマシンに表示されます。Webサイトのセキュリティ証明書に問題があることがユーザに通知されるが、ユーザはWebサイトを継続できる(デフォルト)。
- **Revoked server certificate (validate CRL)**:
  - 選択すると、セキュリティゲートウェイは各サーバのサイト証明書を検証します。セキュリティゲートウェイは、オンライン証明書ステータスプロトコル(OCSP)標準を使用して証明書を検証します。OCSPは、R80.10より下位のリリースで証明書の検証に使用される証明書失効リスト(CRL)検証よりも高速で、メモリ使用量もはるかに少なくすみます。
  - クリアすると、セキュリティゲートウェイはサーバサイト証明書の失効をチェックしません。

  OCSPがサーバ証明書に対してサポートされていない場合、セキュリティゲートウェイはCRL検証を使用します。CRLに到達できない場合、その証明書は信頼されているとみなされます。これはデフォルトの設定です。CRLに到達できなかったことを示すHTTPSインスペクションログが発行されます。

  この動作はデータベースツール(GuiDBEdit Tool)で変更できます:

  手順

  重要 - この変更は、HTTPSインスペクションが有効になっているすべてのセキュリティゲートウェイに適用されます。

  1. SmartConsoleのウィンドウをすべて閉じます。
  2. 接続*Database Tool (GuiDBEdit Tool)*を管理サーバに接続します。
  3. 左上のパネルで、**Other** > **ssl_inspection**をクリックします。
  4. 右上のパネルで、**general_confs_obj and change**をクリックします。
  5. 下のパネルで、属性**drop_if_crl_cannot_be_reached**を右クリック > **Edit**をクリックします。
  6. 値を **"false"** から **"true"** に変更 >**OK**をクリックします。
  7. 上部から、**File**メニューをクリックし、**Save All**をクリックします。

8. データベースツール(GuiDBEditツール) を閉じます。
9. SmartConsoleで管理サーバに接続します。
10. アクセスコントロールポリシーをインストールします。

CRLを検証するには、セキュリティゲートウェイがインターネットに接続可能である必要があります。たとえば、組織環境でプロキシサーバが使用されている場合は、このプロキシサーバを使用するようにセキュリティゲートウェイを設定する必要があります。

セキュリティゲートウェイのプロキシサーバを設定するには

オプションで、SmartConsoleのグローバルプロパティで設定したデフォルトのプロキシサーバを使用することもできます。

1. SmartConsoleのゲートウェイ&サーバビューで、プロキシ設定が必要なセキュリティゲートウェイをダブルクリックします。
2. **Network Management** >**Proxy** にアクセス。
3. **Use custom proxy settings for this network object**と**Use proxy server**を選択し、プロキシIPアドレスを入力します。
4. クリック**OK**。
5. アクセスコントロールポリシーをインストールします。

重要 - セキュリティゲートウェイからの発信HTTPを許可するルールがルールベースにあることを確認してください。

- **Expired Server Certificate**
  - 選択すると、サーバ証明書の有効期限が切れた場合、セキュリティゲートウェイは接続を切断します。
  - クリアされると、セキュリティゲートウェイは有効期限の切れた証明書を作成します。ユーザはWebサイトにアクセスできます(デフォルト) 。
- **Track validation errors**

  サーバ検証をログに記録するか(SmartConsoleの [ログとイベント] ビュー > **Logs**でログを確認) 、他の通知をトリガするかを選択します。

証明書ブロック

ブロックされている証明書のリストを作成できます。これらの証明書を使用しているサーバからのトラフィックはドロップされます。リスト内の証明書がTrusted CAリストにもある場合、ブロック証明書リストはTrusted CAリストを優先します。

- **New**- 証明書を追加できます。証明書のシリアル番号(16進数形式HH:HH) と、証明書を説明するコメントを入力します。
- **Edit**- ブロックされた証明書リストの詳細を変更できます。

- **Delete**- ブロックされた証明書リストから証明書を削除できます。
- **Search**- ブロックされた証明書リストから証明書を検索できます。
- **Track dropped traffic**- サーバ検証をログに記録するか(SmartConsoleのログとイベントビュー > **Logs**でログを確認) 、他の通知をトリガするかを選択します。

許可リストをバイパス

Check Pointは、接続性を向上させるためにバイパス可能な、既知のアップデートサービスおよび証明書ピン留めアプリケーションのリストを動的に更新します。

- **Well-known update services**- いくつかの有名な更新サービスは、正しく機能するためにバイパスする必要があります。更新されたサービスのリストについてはsk98655を参照してください。
- **Certificate-pinned Applications**- モバイルアプリケーションやデスクトップアプリケーションの中には、特定のサーバ証明書だけを信頼するものがあります。このようなアプリケーションは、HTTPSインスペクションのアウトバウンドCA証明書によって署名された証明書が提示された場合、信頼の問題により接続を終了する可能性があります。証明書ピン留めアプリケーションとして分類されるクライアントからの接続が検出されると、選択されたアクションが実行されます。

利用可能なアクション:

アクション	アクション説明
Bypass	HTTPSインスペクションは、中断のない接続性を確保するためにバイパスされ、バイパスログが送信されます。
Detect	HTTPSインスペクションはバイパスされず、検出ログが送信されます。アプリケーションにエラーや不具合が表示される場合があります。
None	HTTPSインスペクションはバイパスされず、専用のログは送信されません。アプリケーションにエラーや不具合が表示される場合があります。

セッションログ

R82以降、セキュリティゲートウェイはセッションログを送信できるようになり、セキュリティゲートウェイを通過するTLSトラフィックの概要を視覚的に把握できるようになりました。

セキュリティゲートウェイがこれらのログを送信できるようにするには

1. **Send session logs**を選択します。
2. HTTPSインスペクションルールベースで、該当するルールの**Track**カラムを**Log**に設定します。

HTTPSインスペクションのセッションログは、いくつかの共通の特徴に基づいて、個々の接続をセッションログにグループ化します。

- ソースIP
- 宛先IP
- SNI(サーバ名表示)
- HTTPSインスペクションアクション:トラフィックをバイパスするかインターセプトするか。
- バイパス理由:トラフィックがバイパスされた場合にのみ適用されるアプリケーション。
- タイムウィンドウ:同じ3時間以内に発生した接続。

これらの特徴を持つ接続を集約することで、セッションログはBypassやInspectの決定を含む統計ビューを作成するために使用されます。詳細については、以下を参照してください。*HTTPSインスペクション統計ビュー (567ページ)*。

その他

中間CA

Use the "Certificate Authority Information Access" extension to retrieve certificates that are missing from the certificate action。

中間CA証明書を自動的に取得:

- このオプションを選択すると、証明書チェーンに含まれない、信頼できるルートCA証明書が発行した中間CA証明書が、証明書の情報を使用して自動的に取得されます(デフォルト)。
- クリアされた場合、中間CAによって署名され、証明書チェーンの一部として送信されないWebサーバ証明書は、信頼されていないとみなされます。

負荷状態のバイパスをログ記録

Bypass Under Loadのログタイプを設定するには

1. **Security Policies** > HTTPSインスペクション > **Inbound Policy** または**Outbound Policy**
2. **HTTPS Inspection Tools**セクションで、**Advanced Settings**をクリックします。
3. **Other**をクリックします。
4. **Bypass Under Load Logging**セクションの**Track**フィールドで、該当するオプションを選択します。
5. **OK**をクリックします。
6. アクセスコントロールポリシーをインストールします。

HTTPSインスペクション統計ビュー

R82以降では、HTTPSインスペクションの統計情報は、[ログとイベント]ビューおよびSmartViewで表示できます。HTTPSインスペクション統計ビューは、バイパス統計と検査統計を含め、セキュリティゲートウェイを通過するHTTPSトラフィックの概要を視覚的に表示します。統計ビューは、セキュリティゲートウェイがセッションログを送信するたびに更新されます。参照：*セッションログ (565ページ)*)。

設定

1. **管理サーバまたはログサーバで必要なSoftware Bladesを有効にする**

    a. SmartConsoleで管理サーバに接続します。

    b. 左のナビゲーションパネルで、ゲートウェイ&サーバビューに移動します。

    c. セキュリティゲートウェイがログを送信する管理サーバまたはログサーバのオブジェクトをダブルクリックします。

    d. 左のパネルで、**General Properties**をクリックします。

    e. **Management**タブで、これらのSoftware Bladesを選択します：

    - **Logging & Status**
    - **SmartEvent Server**
    - SmartEvent相関ユニット

    f. **OK**をクリックして変更を公開します。

    g. 左上隅から、**Menu** > **Install database**をクリックします。

    h. すべてのオブジェクトを選択し、**Install**をクリックします。

    i. 左下でタスクの進行状況をモニタします。

2. **セキュリティゲートウェイでHTTPSインスペクションセッションログを有効にする**

    a. SmartConsoleで、[Manage & Settings]ビュー > **Blades** > HTTPSインスペクション > **Advanced Settings**を開きます。

    HTTPS Inspection - Global Settingsウィンドウが開きます。

    b. 左側のナビゲーションツリーで、**Session Logs**をクリックします。

    c. **Session Logs**を選択して**OK**をクリックします。

HTTPSインスペクション統計の表示

HTTPSインスペクションの統計情報は、この2つの場所で表示できます：

SmartConsole

1. 左のナビゲーションパネルで、ログ&イベントをクリックします。
2. 上部の[+]をクリックすると、新しいタブが開きます。
3. 左側のセクションで、**Views**をクリックします。
4. 上部の検索フィールドに「**HTTPS**」と入力します。
5. **HTTPS Inspection Statistics**というビューをダブルクリックします。

SmartView

1. Webブラウザを使用して、セキュリティゲートウェイがログを送信する管理サーバまたはログサーバのSmartViewポータルに接続します。

   例:

   ```
   https://192.168.22.33/smartview/
   ```

2. 上部の[+]をクリックすると、新しいタブが開きます。
3. 左側のセクションで、**Views**をクリックします。
4. 上部の検索フィールドに次を入力します:**HTTPS**
5. ビューをダブルクリック**HTTPS Inspection Statistics**

ログの詳細を見るには

1. HTTPSインスペクション統計ビューで、該当するグラフまたはチャートをダブルクリックすると、関連するすべてのセッションログが表示されます。
2. 該当するセッションログをダブルクリックすると、関連するすべての接続ログが表示されます(下部のパネルに表示)。
3. 該当する接続ログをダブルクリックすると、ログの詳細が表示されます。

サイト分類のためのSNIサポート

R80.30からは、HTTPSインスペクションを開始する前にHTTPSサイトを分類し、インスペクションが成功しなかった場合に接続が失敗しないようにする新機能が追加されました。

SNIはTLSプロトコルの拡張機能であり、TLSハンドシェイクプロセスの開始時にホスト名を示します。

この分類は、TLSハンドシェーキングプロセスの最初にあるクライアントHelloメッセージのSNIフィールドを調べることによって実行されます。正しいサイトに到達したことを確認するために、SNIは証明書に表示されるホストのSubject Alternative Nameと照合されます。

ホストの身元が判明し確認された後、サイトが分類され、接続を遮断すべきかどうか決定されます。

SNIサポートはデフォルトで有効になっています。

非標準ポートでのHTTPSインスペクション

HTTPを使用するアプリケーションは通常、HTTPトラフィックをTCPポート80に送信します。アプリケーションによっては、他のポートにHTTPトラフィックを送信するものもあります。一部のSoftware Bladeでは、ポート80のHTTPトラフィックのみを検査するように、または非標準ポートのHTTPトラフィックも検査するように設定することができます。

セキュリティポリシーは、たとえ非標準のポートを使って送信されたとしても、すべてのHTTPトラフィックを検査します。このオプションはデフォルトで有効になっています。このオプションは、Manage & Settingsビュー > **Blades > Threat Prevention > Advanced Settings** > **General** > **HTTPS Inspection**で設定できます。この変更を行う場合は、アクセスコントロールポリシーをインストールする必要があります。

TLS v1.3トラフィックのインスペクション

R81以降では、Check Pointセキュリティゲートウェイは、TLS(トランスポートレイヤーセキュリティ) v1.3に依存するトラフィックを遮断できるようになりました(RFC 8446を参照) 。

R81.10以降、この機能は、USFW(ユーザスペースファイアウォール) を使用するセキュリティゲートウェイ(およびクラスタメンバ) に対してデフォルトで有効になります。

対応プラットフォームの一覧はsk167052を参照。

注

- テスト目的でTLS v1.3トラフィックの検査を無効にするには、このコマンドでグローバルパラメータ "`fwtls_enable_tlsio`" の値を`0`に設定します:
  ```
  fw ctl set -f int fwtls_enable_tlsio 0
  ```
- TLS v1.3トラフィックの検査を再び有効にするには、このコマンドでグローバルパラメータ "`fwtls_enable_tlsio`" の値を`1`に設定します:
  ```
  fw ctl set -f int fwtls_enable_tlsio 1
  ```
- セキュリティゲートウェイ/クラスタがHTTP/HTTPSプロキシ(sk110013)として設定されている場合、HTTPSインスペクションはTLS v1.3をサポートしません。

HTTP/3 プロトコルのインスペクション (RFC 9114)

R82以降のCheck Point セキュリティゲートウェイでは、有効なSoftware Bladesの設定に基づき、復号されたインバウンドおよびアウトバウンドのHTTP/3トラフィックを検査できます。

HTTP/3は、TCPの代わりにUDP上で動作するQUICトランスポートプロトコルを使用することで、速度、信頼性、セキュリティを向上させるように設計されたHTTPプロトコルの新バージョンである。HTTP/3プロトコル(RFC 9114)は、QUICでのHTTPセマンティクスの伝送を最適化します。

HTTP/3は、HTTP/2のすべてのコア機能を保持しながら、待ち時間の短縮とパフォーマンスの向上を実現して効率性を高めます。

HTTP/3 over TLSは、安全なTLS接続を介してHTTP/3接続を有効にします。

ベストプラクティス - バージョンR81.20以前のセキュリティゲートウェイでは、sk111754で説明されているようにQUICプロトコルをブロックします。

ルールベースでのHTTPS/3の使用

透過的なQUICインスペクションのために、QUICサービスがデフォルトのHTTPSサービスグループに追加されました。サービス& アプリケーションカラムのアクセスコントロールポリシーと、[Services]カラムのHTTPSインスペクションポリシーで使用できます。

例:

No.	名前	発信元	宛先	サービス	カテゴリ/カスタムアプリケーション	アクション	追跡	ブレード	インストール先
1	QUIC - 「ゲーム」カテゴリをバイパス	*Any	Internet	quic	Games	Bypass	Log	All	Policy HTTPS Targets
2	QUIC - インスペクション	*Any	Internet	quic	Any	Inspect	Log	All	Policy HTTPS Targets

HTTP/3インスペクションのモニタリング

CPViewでセキュリティゲートウェイのHTTP/3インスペクション統計を表示できます:

1. セキュリティゲートウェイのコマンドラインに接続し、次を実行します:

   ```
   cpview
   ```

2. 上部で、**Advanced** > **HTTP-Parser** > **QUIC**をクリックします。

出力例:

```
|-------------------------------------------------------------------
-------------------------------------------------------------------
--------------------|
| CPVIEW.Advanced.HTTP-Parser.QUIC

13Jul2024 16:48:27 |
|-------------------------------------------------------------------
-------------------------------------------------------------------
--------------------|
| Overview SysInfo Network CPU I/O Software-blades Hardware-Health
Management Advanced
                     |
|-------------------------------------------------------------------
-------------------------------------------------------------------
--------------------|
```

```
| Logging CPU-Profiler Memory Network SDWAN SecureXL ClusterXL
CoreXL PrioQ Streaming NAT MUX Routed RAD Conn-Tracker UP HTTP-
Parser SSH-Parser CPAQ       >>
|-------------------------------------------------------------------
-------------------------------------------------------------------
--------------------|
| General HTTP3-Information QUIC

                  |
|-------------------------------------------------------------------
-------------------------------------------------------------------
--------------------|
| Connections overview

                  |
|

                  |
| Processed Connections:                                          0

                  |
| HTTPS Inspection - Inspect:                                     0

                  |
| Website Categorization:                                         0

                  |
| HTTPS Inspection - Bypass on first packet:                      0

                  |
| HTTPS Inspection - Bypass on category/app:                      0

                  |
| Downgraded:                                                     0

                  |
| Closed with error:                                              0

                  |
| -------------------------------------------------------------------
-------------------------------------------------------------------
------------------- |
| Downgrade reasons

                  |
|

                  |
```

```
| QUIC inspection disabled                0

                  |
| Strict Hold is active                   0

                  |
| Exception                               0

                  |
| ------------------------------------------------------------------
------------------------------------------------------------------
------------------- |
| QUIC Errors

                  |
|

                  |
| Error type                                                      #
of errors             # in the last 10 min window
                   |
| Unknown error                                                   0
                     0
                  |
| Transport internal error                                        0
                     0
                  |
| Connection refused                                              0
                     0
                  |
| Flow control violation on stream                                0
                     0
                  |
| Frame exceeding stream limits                                   0
                     0
                  |
| Received frame mismatch with stream state                       0
                     0
                  |
| New final size mismatch with previous final size                0
                     0
                  |
| Could not decode frame                                          0
                     0
                  |
| Bad transport parameters                                        0
                     0
                  |
```

```
| Received connection ID going over the limit                    0
                    0
                  |
| Protocol violation                                             0
                    0
                  |
| Invalid token                                                  0
                    0
                  |
| Connection timeout due to lack of progress                     0
                    0
                  |
| Crypto buffer exceeded crypto level in stream                  0
                    0
                  |
| Key update error                                               0
                    0
                  |
| AEAD limit reached                                             0
                    0
                  |
| No viable path                                                 0
                    0
                  |
| Cannot create control stream: peer-imposed limit               0
                    0
                  |
| HTTP internal error                                            0
                    0
                  |
| Cannot create stream                                           0
                    0
                  |
| Critical stream closed                                         0
                    0
                  |
| Unexpected frame received on stream                            0
                    0
                  |
| Malfored frame: could not parse frame                          0
                    0
                  |
| Excessive load                                                 0
                    0
                  |
| Invalid stream ID                                              0
                    0
                  |
```

```
| Unexpected HTTP/2 setting                                                0
                     0
                   |
| First control frame is not SETTINGS                                      0
                     0
                   |
| Got stream while going away                                              0
                     0
                   |
| Refuse push stream                                                       0
                     0
                   |
| Request is incomplete                                                    0
                     0
                   |
| Parsing error: frame contains invalid headers                            0
                     0
                   |
| Content error                                                            0
                     0
                   |
| Version fallback                                                         0
                     0
                   |
| Stream QPACK decompression error                                         0
                     0
                   |
| Error interpreting QPACK encoder stream                                  0
                     0
                   |
| Error interpreting QPACK decoder stream                                  0
                     0
                   |
| Invalid certificate                                                      0
                     0
                   |
| ------------------------------------------------------------------------
------------------------------------------------------------------------
------------------- |
```

制限事項

- セキュリティゲートウェイがHTTP/3インスペクションをサポートするのは、USFW(ユーザスペースファイアウォール)モードで実行される場合のみです。

  セキュリティゲートウェイは、カーネルモードファイアウォールで動作する場合、HTTP/3トラフィックを以前のHTTPバージョンにダウングレードします。

  USFW(ユーザスペースファイアウォール)モードについては、お使いのバージョンのリリースノートおよびsk167052を参照してください。

- セキュリティゲートウェイは、脅威対策の「ディープインスペクション」モードが有効な場合、HTTP/3トラフィックをドロップします。

- ChromiumベースのWebブラウザは、HTTPSインスペクション証明書がChromiumの信頼リストにある信頼できるCAによって署名されている場合にのみ、HTTP/3トラフィックを許可します。

  ChromiumベースのWebブラウザでは、HTTP/3トラフィックの証明書をブラウザの信頼済みストアに追加できません。sk111754を参照してください。

- プロキシ経由でのQUICトラフィックの検査はサポートされていない。

- HTTP/3以外のすべてのプロトコルは、以前のHTTPバージョンにダウングレードされます。

TLS接続のブロック

セキュリティゲートウェイから内部ネットワークへのインバウンドTLS 1.0およびTLS 1.1接続、内部ネットワークからセキュリティゲートウェイへのアウトバウンドTLS 1.0およびTLS 1.1接続をブロックできます。

事前準備

- 管理サーバR80以上。
- セキュリティゲートウェイR80.10以降。
- アクセスコントロールポリシーでアプリケーションとURLフィルタリングレイヤーを有効にします。
- セキュリティゲートウェイでアプリケーションとURLフィルタリングブレードを有効にします。
- この手順は、これらすべての設定の組み合わせで機能します:

	HTTPSインスペクションが有効	HTTPSインスペクションが無効
HTTPS Web サイトを分類 有効	はい	はい

	HTTPSインスペクションが有効	HTTPSインスペクションが無効
HTTPS Webサイトの分類" 無効	はい	はい

注

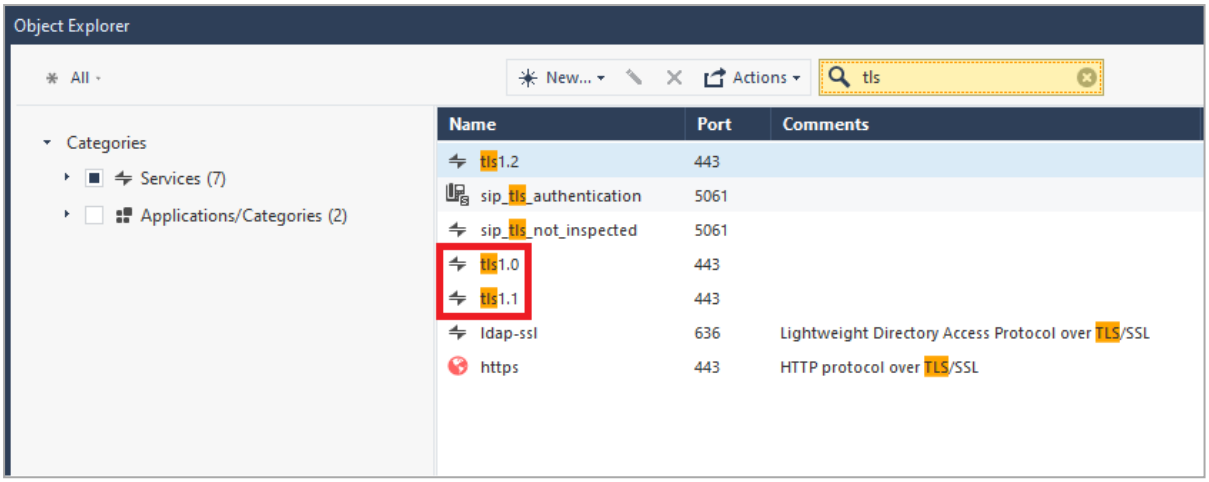
- **HTTPS Webサイトの分類**を有効にするには: SmartConsoleで、[管理と設定]ビュー > **Blades** > **Application Control & URL Filtering**をクリックし、**Advanced Settings** > **URL Filtering** > **Categorize HTTPS websites**を選択します。
- HTTPSインスペクションを有効にするには: SmartConsole で、ゲートウェイ&サーバビューに移動し、必要なセキュリティゲートウェイまたはセキュリティクラスタオブジェクトをダブルクリックし、セキュリティゲートウェイまたはセキュリティクラスタ エディタで、HTTPSインスペクションページに移動し、**Enable HTTPS Inspection**を選択します。
- HTTPSインスペクションが有効な場合、TLS 接続のブロックはKSFW(カーネルスペースファイアウォール)とUSFW(ユーザスペースファイアウォール)の両方で機能します。これらのファイアウォールのモードについては、sk167052を参照してください。

手順

パート1 - ユーザ定義サービスの作成

1. SmartConsoleを使用して、このセキュリティゲートウェイを管理するSecurity Management ServerまたはドメインManagement Serverに接続します。
2. SmartConsoleの右上隅で、**Objects**、アイコンをクリックすると、**Object Explorer**ウィンドウが開きます。
3. 一番上の検索フィールドで、次のように検索します:

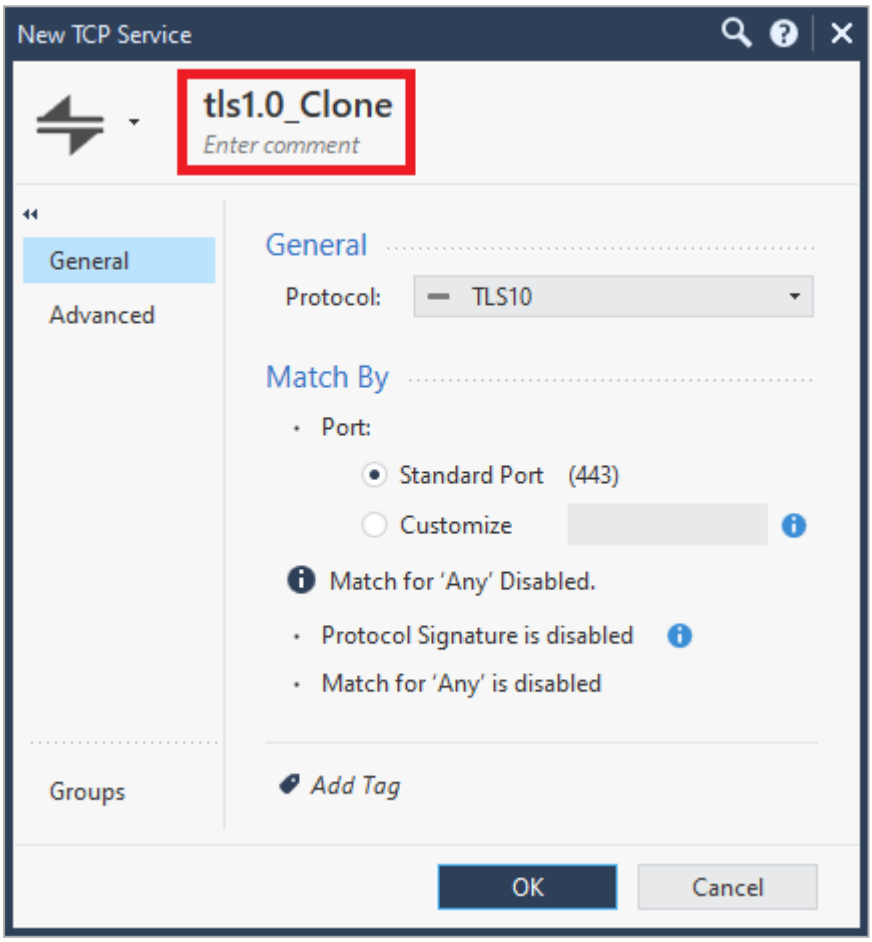
   tls



4. TLS 1.0接続をブロックするには

   a. 定義済みサービス**tls1.0**を右クリックし、**Clone**をクリックします。

      New TCP Serviceウィンドウが開きます。



b. **Name**フィールドで、名前を「**tls1.0_Clone**」から必要な名前に変更します。

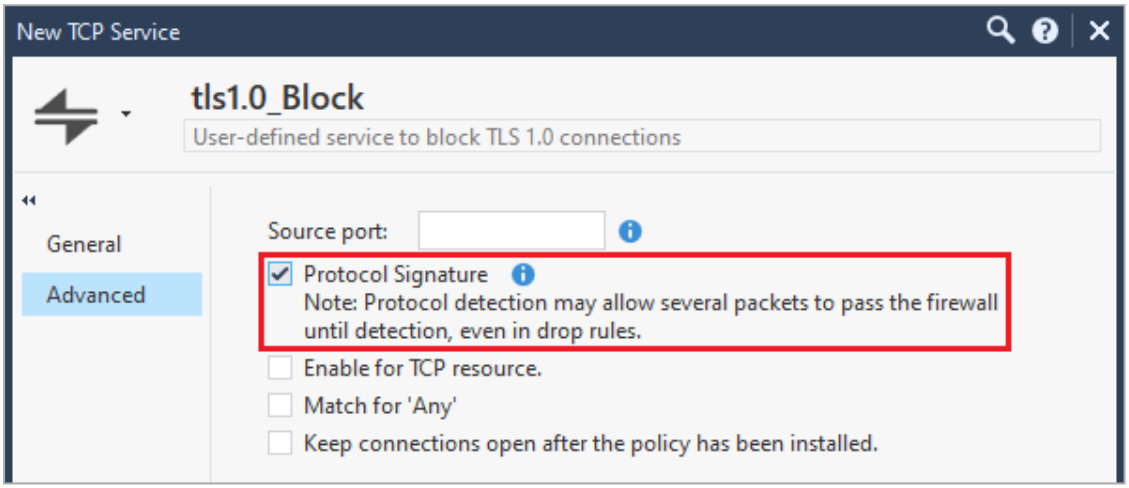
例：**tls1.0_Block**

c. オプション：**Comment**フィールドに、該当するテキストを入力します。

例：TLS 1.0接続をブロックするユーザ定義サービス

d. 左のパネルで、**Advanced**をクリックします。

e. 上部のセクションで、**Protocol Signature**を選択します。

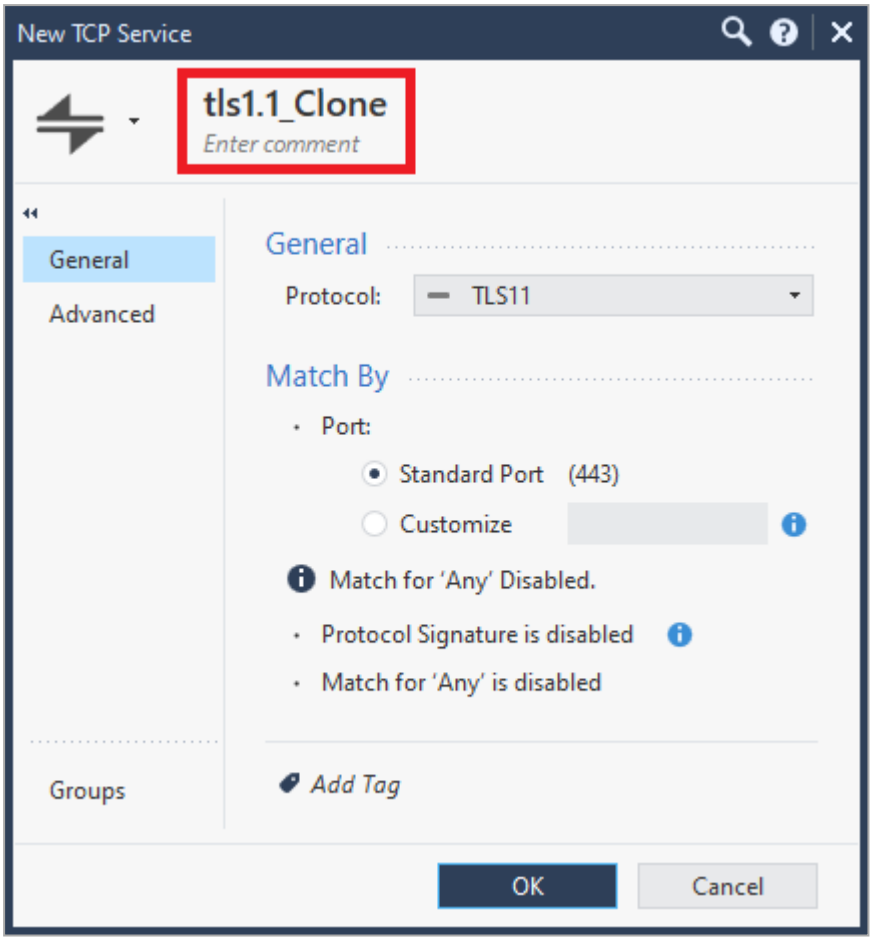


f. **OK**をクリックします。

5. TLS 1.1接続をブロックするには

a. 定義済みサービス**tls1.1**を右クリックし、**Clone**をクリックします。

New TCP Serviceウィンドウが開きます。



b. **Name**フィールドで、名前を「**tls1.1_Clone**」から必要な名前に変更します。

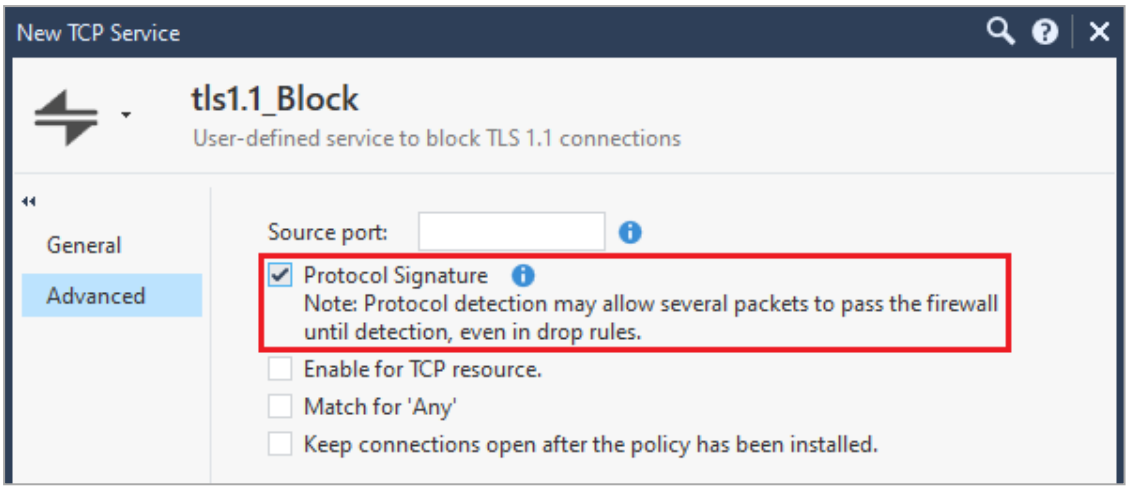
例：**tls1.1_Block**

c. オプション：**Comment**フィールドに、該当するテキストを入力します。

例：TLS 1.1接続をブロックするユーザ定義サービス。

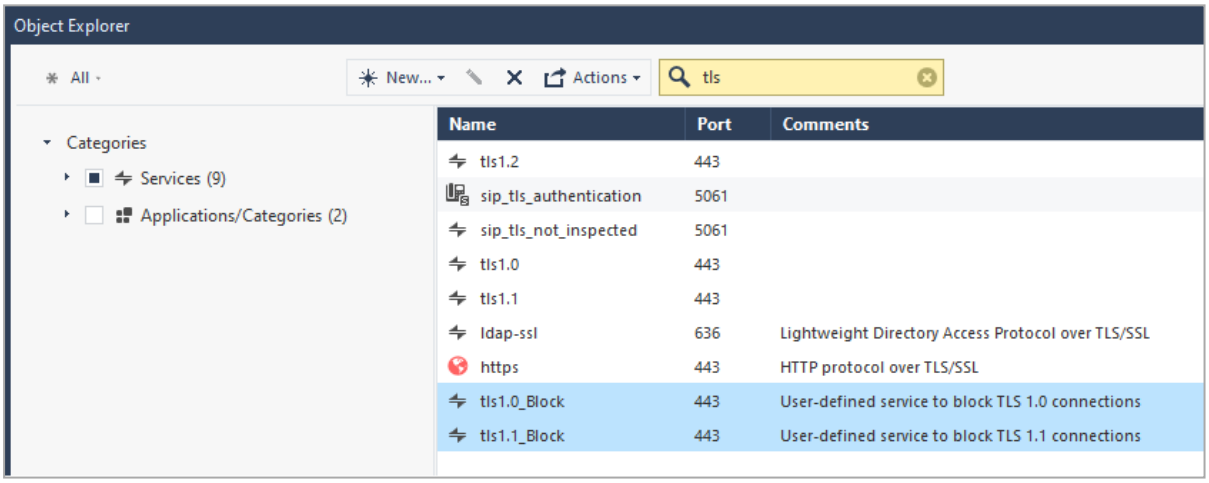
d. 左のパネルで、**Advanced**をクリックします。

e. 上部のセクションで、**Protocol Signature**を選択します。



f. **OK**をクリックします。

結果の例：



6. オブジェクトエクスプローラウィンドウを閉じます。

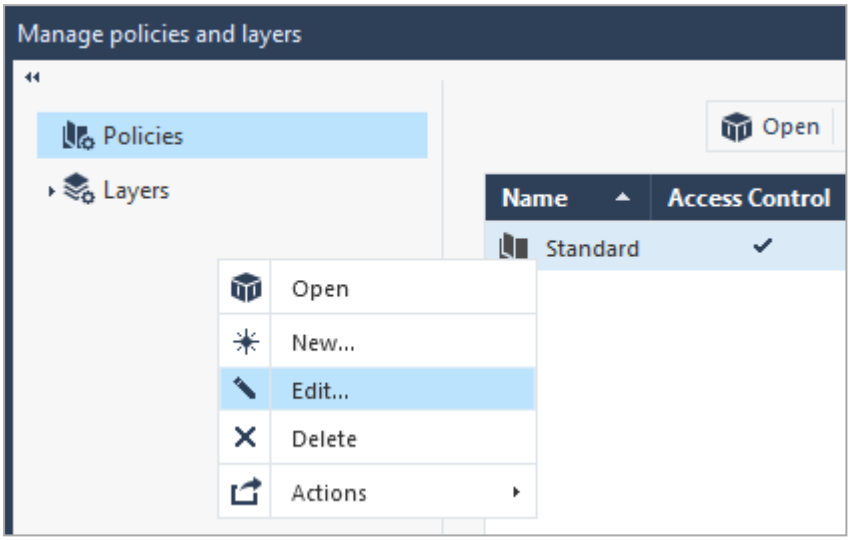
パート2 - セキュリティゲートウェイの設定

1. SmartConsoleで、ゲートウェイ＆サーバビューに移動します。
2. 該当するセキュリティゲートウェイまたはセキュリティクラスタオブジェクトをダブルクリックします。

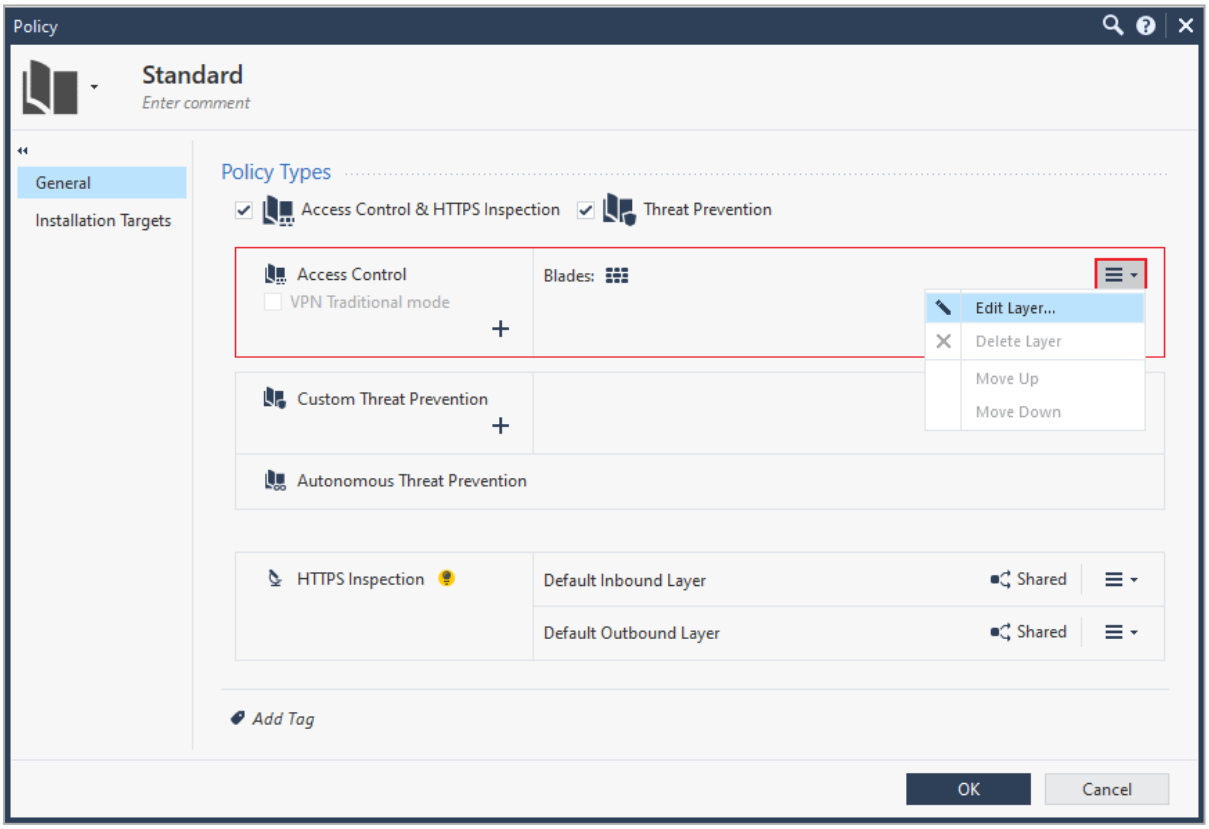
   セキュリティゲートウェイまたはセキュリティクラスタエディタが開きます。
3. **General Properties**ページで**Network Security**タブを開きます。
4. Application Control Software Bladeを選択します。
5. **OK**をクリックします。

パート3 - アプリケーションとURLフィルタリングレイヤーを有効にする

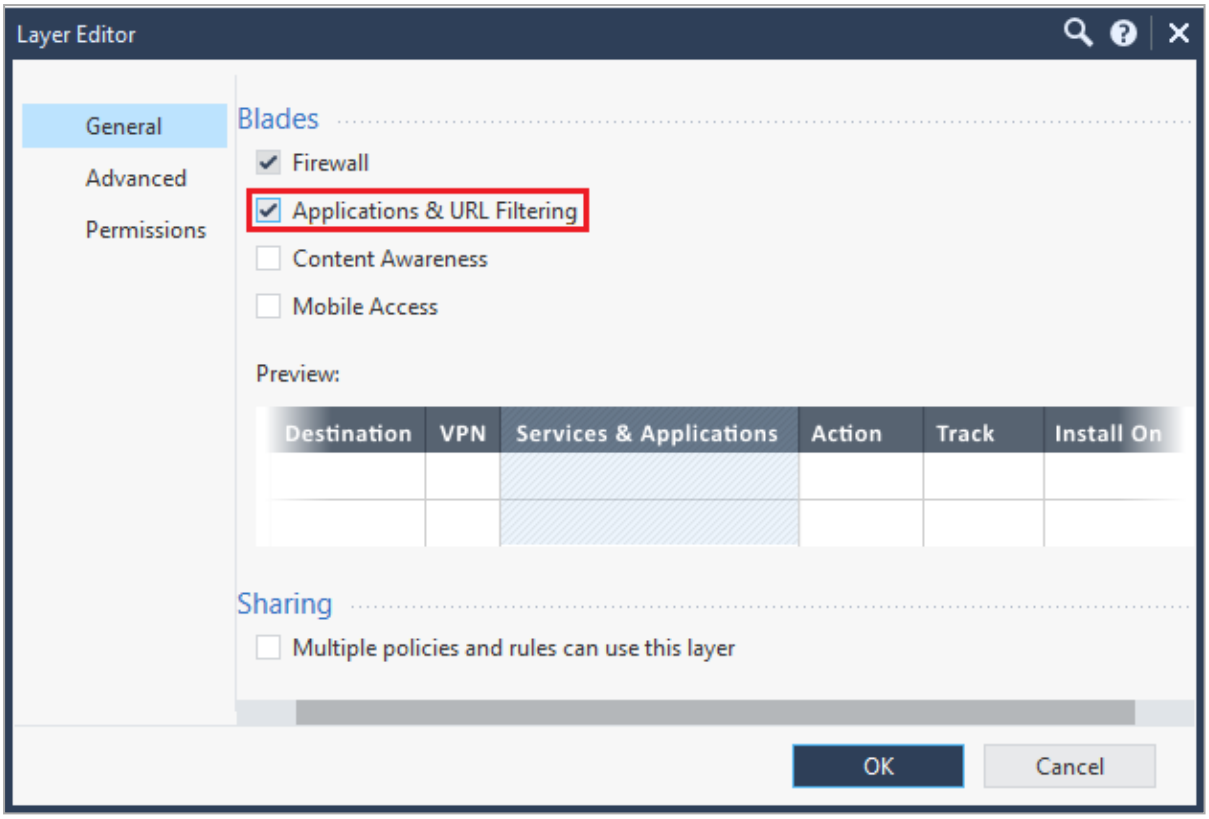
1. SmartConsoleの左上でをクリックし、**Manage policies and layers**を選択します。
2. セキュリティゲートウェイまたはセキュリティクラスタにインストールした該当するポリシーを右クリックし、**Edit**をクリックします。



3. アクセスコントロールの行で、右上隅のをクリックし、**Edit Layer**を選択します。



4. **General**ページの**Blades**セクションで、**Application & URL Filtering**を選択します。



5. **OK**をクリックして**Layer Editor**ウィンドウを閉じます。
6. **OK**をクリックして**Policy**ウィンドウを閉じます。
7. **Manage policies and layers** ウィンドウを閉じます。

パート4 - アクセスコントロールポリシーの設定

1. SmartConsoleの左のナビゲーションパネルで、セキュリティポリシーをクリックします。
2. アクセスコントロールセクションで、**Policy**をクリックします。
3. TLS 1.0およびTLS 1.1接続をブロックする新しいルールを追加します:

名前	発信元	宛先	VPN	サービス&アプリケーション	内容	アクション	追跡
TLS 1.0のブロック	該当ソース	該当する宛先	*Any	ユーザ定義サービス tls1.0_Block	*Any	Drop	LogまたはNone

名前	発信元	宛先	VPN	サービス&アプリケーション	内容	アクション	追跡
TLS 1.1のブロック	該当ソース	該当する宛先	*Any	ユーザ定義サービス tls1.1_Block	*Any	Drop	LogまたはNone

4. セッションを公開します。
5. セキュリティゲートウェイまたはセキュリティクラスタオブジェクトにアクセスコントロールポリシーをインストールします。

スマートフォンとタブレット向けクライアント証明書

ユーザが携帯デバイスを使用してリソースにアクセスできるようにするには、クライアント証明書を使用してセキュリティゲートウェイに認証できることを確認します。

多くの組織では、クライアント証明書の割り当てや管理の日常業務は、セキュリティゲートウェイを管理する部署とは別の部署が行っています。たとえば、コンピュータのヘルプデスクなどです。SmartConsoleを使用してクライアント証明書を作成することを許可する管理者を作成し、他の権限を制限することができます (*クライアント証明書に対する権限の付与 (589ページ)*)。

クライアント証明書を設定するには、SmartConsoleを開き、**Security Policies** >**Access Control** >**Access Tools** >**Client Certificates** にアクセスします。

モバイルアクセスポリシーを設定するには、**Manage & Settings** >**Blades** >**Mobile Access** >**Configure in SmartDashboard** にアクセスします。SmartConsoleの**Client Certificates**ページは、SmartDashboardの**Mobile Access**タブ、**Client Certificates**ページへのショートカットです。

クライアント証明書の管理

モバイルデバイス向けのCheck Point Mobile Appsでは、証明書のみの認証、またはクライアント証明書とユーザ名/パスワードによる2要素認証を使用できます。この証明書は、モバイルアクセスセキュリティゲートウェイを管理するSecurity Management Serverの内部CAによって署名されています。

Security Policies >**Access Control** >**Access Tools** >**Client Certificates** でクライアント証明書を管理します。

ページには2つのペインがあります。

- **Client Certificates**ペインでは:
  - クライアント証明書の作成、編集、失効を実行します。
  - すべての証明書、そのステータス、有効期限、登録キーを確認します。デフォルトでは、最初の50件だけが証明書リストに表示されます。**Show more**をクリックすると、多くの結果が表示されます。
  - 指定した証明書を検索します。
  - ユーザへ証明書情報を送信します。
- **Email Templates for Certificate Distribution**ペインでは:
  - クライアント証明書配布用のメールテンプレートを作成および編集します。
  - メールテンプレートのプレビュー。

クライアント証明書の作成

注 - LDAPまたはADを使用している場合、クライアント証明書を作成しても、LDAPまたはADサーバは変更されません。LDAP/ADの書き込みアクセスに関するエラーメッセージが表示された場合は、無視してウィンドウを閉じて続行してください。

クライアント証明書ウィザードで証明書を作成および配布するには

1. SmartConsoleで、**Security Policies** >**Access Control** >**Access Tools** >**Client Certificates** を選択します。
2. **Client Certificates**ペインで、**New**をクリックします。

   Certificate Creation and Distributionウィザードが開きます。
3. **Certificate Distribution**ページで、登録キーをユーザに配布する方法を選択します。どちらか一方、または両方を選択することができます。
   a. **Send an email containing the enrollment keys using the selected email template**- 各ユーザは、選択したテンプレートに基づいて、登録キーを含むEメールを受け取ります。
      - **Template**- 使用するEメールテンプレートを選択します。
      - **Site**- ユーザが接続するセキュリティゲートウェイを選択します。
      - **Mail Server**- メールを送信するメールサーバを選択します。

      Edit をクリックすると、その詳細が表示され、変更することができます。
   b. **Generate a file that contains all of the enrollment keys**- 全ユーザのリストと登録キーを含む記録用コンテナファイルを作成します。
4. **オプション:** 登録キーの有効期限を変更するには、**Users must enroll within x days**で日数を編集します。
5. **オプション: Client Certificates**ページの証明書リストの証明書の横に表示されるコメントを追加します。
6. クリック**Next**。

   Usersページが開きます。
7. **Add**をクリックして、証明書を必要とするユーザまたはグループを追加します。
   - 検索フィールドにテキストを入力し、ユーザまたはグループを検索します。
   - グループの種類を選択し、検索を絞り込むことができます。
8. 含まれるすべてのユーザまたはグループがリストに表示されたら、**Generate**をクリックして、証明書を作成し、メールを送信します。
9. 10個以上の証明書を生成する場合は、**Yes**をクリックして、続行することを確認します。

進捗ウィンドウが表示されます。エラーが発生した場合は、エラーレポートが開きます。

10. クリックFinish。
11. クリックSave。
12. SmartConsoleでポリシーをインストールします。

証明書の取り消し

証明書のステータスがPending Enrollmentの場合、証明書を取り消すと、Client Certificateリストに表示されなくなります。

1つ以上の証明書を失効させるには

1. Client Certificateリストから、1つまたは複数の証明書を選択します。
2. Revokeをクリックします。
3. クリックOK。

証明書を取り消すと、Client Certificateリストに表示されなくなります。

証明書配布用のテンプレートの作成

Eメールテンプレートを作成または編集するには

1. SmartConsole で、Security Policies >Access Control >Access Tools >Client Certificates を選択します。
2. 新しいテンプレートを作成するにはEmail Templates for Certificate Distributionペインで、Newを選択します。

   テンプレートを編集するにはEmail Templates for Certificate Distributionペインでテンプレートをダブルクリックします。

   Email Templateが開きます。
3. テンプレートのNameを入力します。
4. **オプション:** Commentを入力します。コメントは、Client Certificatesページのメールテンプレートリストに表示されます。
5. **オプション:** メールの言語を変更するにはLanguagesをクリックします。
6. EメールのSubjectを入力します。Insert Fieldをクリックして、ユーザ名などの定義済みフィールドを追加します。

7. メッセージの本文にテキストを追加して書式設定します。**Insert Field**をクリックして、ユーザ名、登録キー、有効期限などの定義済みフィールドを追加します。
8. メールテンプレート本文の中をクリックします。
9. **Insert Link**をクリックし、追加するリンクの種類(リンクまたはQRコード)を選択します。

   - **サイトと証明書の作成**

     すでにCheck Pointアプリがインストールされているユーザ向けです。

     ユーザがQRコードを読み取るまたはリンクをクリックすると、サイトが作成され、証明書が登録されます。

     サイトに接続するクライアントの種類を選択 - ユーザがインストールするクライアントの種類を1つ選択します。

     - **Capsule Workspace**- モバイルデバイス上に安全なコンテナを作成し、ユーザが社内Webサイト、ファイル共有、Exchangeサーバにアクセスできるようにするアプリ。
     - **Capsule Connect/VPN**- すべてのモバイルアプリケーションへのネットワークアクセスをユーザに提供する、完全なレイヤー3トンネルアプリケーション。

   - **ダウンロード**

     モバイルデバイス用のCheck Pointアプリをダウンロードするよう、ユーザに指示します。

     クライアントデバイスのOSを選択します。

     - **iOS**
     - **Android**

     サイトに接続するクライアントの種類を選択 - ユーザがインストールするクライアントの種類を1つ選択します。

     - **Capsule Workspace**- モバイルデバイス上に安全なコンテナを作成し、ユーザが社内Webサイト、ファイル共有、Exchangeサーバにアクセスできるようにするアプリ。
     - **Capsule Connect/VPN**- すべてのモバイルアプリケーションへのネットワークアクセスをユーザに提供する、完全なレイヤー3トンネルアプリケーション。

   - **カスタムURL**

     独自のURLを設定できます。

リンクタイプごとに、メールテンプレートに追加する要素を選択できます。

- **Link URL**- 完全なリンクアドレスを入力します。
- **QR Code**- 有効にすると、ユーザはモバイルデバイスでコードをスキャンします。
- **HTML Link**- 有効にすると、ユーザはモバイルデバイスでリンクをタップします。

  QR Codeと**HTML Link**を選択してメールに両方含めることができます。
- **Display Text**- リンクタイトルのテキストを入力します。

10. クリック**OK**。
11. **オプション: Preview in Browser** をクリックすると、メールのプレビューが表示されます。
12. クリック**OK**。
13. 変更内容を公開します。

テンプレートの複製

Eメールテンプレートを複製して、既に存在するテンプレートと類似したテンプレートを作成します。

メールテンプレートのクローンを作成するには

1. **Client Certificates**ページのテンプレート一覧から、テンプレートを選択します。
2. **Clone**をクリックします。
3. 選択したテンプレートの新しいコピーが開き、編集することができます。

クライアント証明書に対する権限の付与

SmartConsoleを使用してクライアント証明書を作成し、その他の権限を制限することができる管理者を作成できます。

クライアント証明書の管理者を作成するには

1. 管理者を定義します (*管理者アカウントの管理 (74ページ)*
2. クライアント証明書を扱う権限を持つ、管理者用のカスタマイズされたプロファイルを作成します。管理者プロファイルの**Others**ページで設定します。その他の権限を制限する (*管理者への権限プロファイルの割り当て (116ページ)*)。

環境設定と管理設定

ここでは、SmartConsoleの各種設定について説明します。

データベースの改訂

Security Managementのアーキテクチャには、リビジョンが組み込まれています。各公開操作では、以前のリビジョンからの変更点のみを含む新しいリビジョンが作成されます。

リビジョンアーキテクチャーの利点：

- 障害からの安全なリカバリ、データベースを良好なリビジョンに復元することが可能。
- インストールされたバージョン間の差異に基づく、迅速なポリシーの検証
- より効率的なマネジメント ハイアベイラビリティ。

重要 - リビジョン機能を使用する前に、以下の制限を考慮してください。

- Backup Security Management Serverでは、データベースのリビジョンを戻す操作はサポートされていません。
- 以前のリビジョンに戻すことは不可逆的な操作です。ターゲットリビジョンより新しいバージョンは失われます。
- 変更はオブジェクトにのみ適用され、ファイルシステムには反映されません。
- タスク、SIC、ライセンスは元に戻りません。
- 元に戻すアクションは、他の接続されているすべてのユーザを切断し、それらのプライベートセッションをすべて破棄します。
- リビジョンは、次のシナリオではサポートされません。
  - Endpoint Security Management Server。
  - SmartConsoleとSecurity Management Serverがプロキシサーバを介して接続されている場合、この機能のGUIはサポートされません。この場合、該当するAPIコマンドを使用します。
  - VSXの設定または関連するネットワークがソースとターゲットのリビジョン間で異なっている場合。
  - Multi-Domain Server、Security Management Server、またはCheck Pointオブジェクトのいずれかが、対象改訂日以降に新規作成または削除された場合。
  - グローバルドメイン、またはIPSやアプリケーションコントロールのコンポーネントの対応するリビジョンがパージされた場合。
- 以前のリビジョンに戻すと、ネイティブクラウドによるサイト間VPNトンネルの構成は保存されません。(*R82 Site to Site VPN Administration Guide*> *ネイティブクラウドによるシームレスなサイト間VPNトンネル)*。

ベストプラクティス:

1. リバート後に、IPSとアプリケーションコントロールのシグネチャを更新し、ポリシーをインストールすることをお勧めします。ログ宛先の変更が適用される場合は、ポリシーをインストールします。
2. ある時点までの環境の完全な復元が必要な場合は、**Restore Backup**を使用します。バックアップ後に行った作業はすべて失われます。詳細:*R82 Gaia Administration Guide*
3. 不要なリビジョンはパージすることをお勧めします。あまりに多くのリビジョンを残すと、サーバに大きな負荷がかかり、ディスクやパフォーマンスの問題が発生する可能性があります。

保存されたデータベースのバージョンを見るには

SmartConsoleのManage & Settings >**Sessions** >**Revisions**を開きます。

特定のリビジョンを開くには

1. **Manage & Settings > Sessions > Revisions**にアクセスし、リビジョンを選択します。

   下のペインには、リビジョンで行われた変更の監査ログが表示されます。

2. **オプション: View**をクリックします。

   読み取り専用のSmartConsoleセッションが別に開きます。

2つのリビジョンを比較するには

1. SmartConsoleのManage & Settings >**Sessions** >**Revisions**を開きます。
2. リビジョンを選択します。
3. ツールバーで、**Changes**をクリックします。
4. 比較するリビジョンを選択します。
   - 現在のリビジョン

     または

   - リスト内の以前のリビジョン。このオプションを選択した場合は、リストから該当するリビジョンを選択します。

   変更レポートが作成されます。レポートには、選択した2つのリビジョンの比較が表示されます。

以前のリビジョンに戻すには

1. **Manage & Settings > Sessions > Revisions**にアクセスし、リビジョンを選択します。
2. **Actions**で、**Revert to this Revision**をクリックします。

Revert to Revisionウィザードが開きます。

選択したバージョンより古いバージョンのデータベースをすべて削除するには

1. **Manage & Settings > Sessions > Revisions**にアクセスし、リビジョンを選択します。
2. **Actions**で、**Purge**をクリックします。
3. 表示された確認ウィンドウで、**Yes**をクリックします。

重要 - パージは元に戻せません。パージすると、そのリビジョンと古いリビジョンが削除されます。

注：

- SmartConsoleでセキュリティ管理サーバに接続している場合、システムドメイン内のManagement APIで公開されたセッションは、**Revisions**のビューに表示されません。
- 管理APIを使用してSecurity Management Serverのドメインに接続し、*view-published-sessions*を*true*に設定して*show sessions* APIコマンドを実行すると、システムドメインの変更が含まれていても、SmartConsoleを介して公開されたセッションが返されないという問題がありました。

環境のIPアドレスバージョンの設定

多くのオブジェクトやルールでIPアドレスが使用されています。お使いの環境で使用するバージョンを設定し、関連するオプションのみを表示するようにします。

IPアドレスのバージョンを設定するには

1. **Manage & Settings**をクリックします。
2. **Preferences**をクリックします。
3. お使いの環境で使用しているIPアドレスのバージョンを選択します(**IPv4**、**IPv6**、**IPv4 and IPv6**) 。
4. サブネットの表示方法を選択します(**Mask Length**または**Subnet Mask**) 。

ウィンドウのデフォルト復元

SmartConsoleの一部のウィンドウには、管理者がウィンドウを再表示しないようにするオプションがあります。この選択を元に戻すと、すべてのウィンドウが再び表示されるように復元できます。

このオプションは、管理者がウィンドウでDo not showを選択した場合にのみ利用できます。

ウィンドウを「表示しない」から復元するには

1. Manage & Settingsをクリックします。
2. Preferencesをクリックします。
3. User Preferences領域で、Restore All Messagesをクリックします。

ログインウィンドウの設定

運用環境では、管理者が毎日SmartConsoleを使用します。ログイン画面をカスタマイズし、企業文化に合った環境を設定することができます。

ログインウィンドウをカスタマイズするには

1. **Manage & Settings**をクリックします。
2. **Preferences** >**Login Message** をクリックします。

   Login Messageウィンドウが開きます。
3. **Show custom message during login**を選択します。
4. **Customize Message**に、管理者が見ることができるように**Header**と**Message**を入力します。

   デフォルトの提案:
   ```
   Warning
   This system is for authorized use only
   ```
5. メッセージに警告アイコンを表示させたい場合は、**Customize Layout**で、**Add warning sign**を選択します。
6. ログインウィンドウに組織のロゴを表示させたい場合は、**Customize Layout**で**Add logo**を選択し、画像ファイルを選択(**Browse**)します。

ユーザセンターとの同 期

セキュリティゲート ウェイの名 前 、バージョン、有 効なブレードなど、ユーザ環 境に関 する情 報をユーザセンターへ追 加 することができます。Check Pointは、この追 加 情 報を在 庫 管 理 、積 極 的なサポート 、およびチケット の効 率 的な解 決 に活 用します。

詳しくは、sk94064をご覧ください。

User Centerと同 期 するには

1. SmartConsoleで、**Manage & Settings**をクリックします。
2. クリック**Sync with User Center**
3. **Synchronize information once a day**を選 択します。

インスペクションの設定

セキュリティゲートウェイのインスペクションを設定できます。

- ディープパケットインスペクションの設定
- プロトコル解析のインスペクション設定
- VoIPパケットインスペクションの設定

Security Management Serverには、セキュリティゲートウェイ向けに事前に設定された2つのインスペクションプロファイルが備えられています。

- **Default Inspection**
- **Recommended Inspection**

セキュリティゲートウェイを設定すると、そのセキュリティゲートウェイに対して**Default Inspection**プロファイルが有効化されます。また、**Recommended Inspection**プロファイルをセキュリティゲートウェイに割り当てるか、またはカスタムプロファイルを作成してセキュリティゲートウェイに割り当てることも可能です。

インスペクション設定を有効にするために、アクセスコントロールポリシーをインストールします。

注 - SmartDashboard R77.30 以下では、**Inspection Settings** は**IPS Protections** として設定されます。

インスペクションの設定

インスペクション設定を行うには

1. SmartConsoleで、**Manage & Settings** >**Blades**ビューにアクセスします。
2. **General**セクションで、**Inspection Settings**をクリックします。

   Inspection Settingsウィンドウが開きます。

以下を実行できます。

- インスペクション設定を編集する。
- ユーザが定義した**インスペクション設定**プロファイルを編集する。**Default Inspection**プロファイルと**Recommended Inspection**プロファイルは変更できません。
- セキュリティゲートウェイに**インスペクション設定**プロファイルを割り当てる。
- 例外を設定する。

設定を編集するには

1. **Inspection Settings** >**General** ビューで、設定を選択します。
2. クリック**Edit**。
3. 開いたウィンドウで、プロファイルを選択し、**Edit**をクリックします。

   設定画面が表示されます。
4. 次を選択します:**Main Action:**
   - **Default Action**- 設定済みアクション
   - **Override with Action**-ドロップダウンメニューから、デフォルトをオーバーライドするアクションを選択します - **Accept**, **Drop**, **Inactive** (設定は無効になっています)
5. 設定:**Logging Settings**

   ドロップルールでブロックされたパケットを調べることができるようにする場合は、**Capture Packets**を選択します。
6. クリック**OK**。
7. クリック**Close**。

SYN攻撃の高度な設定については[sk120476]を参照してください。

特定のプロファイルの設定を表示するには

1. **Inspection Settings** >**General** ビューで、**View** > **Show Profiles**をクリックします。
2. 開いたウィンドウで、**Specific Inspection settings profiles**を選択します。
3. プロファイルを選択します。
4. クリック**OK**。

   選択したプロフィールの設定値のみ表示されます。

カスタムのインスペクション設定プロファイルを追加、編集、削除することができます。

カスタムインスペクション設定プロファイルを編集するには

1. **Inspection Settings** > **Profiles**ビューで、プロファイルを選択します。
2. **Delete**をクリックすると削除され、**Edit**をクリックするとプロファイル名、関連する色、またはタグが変更されます。
3. プロファイル属性を編集した場合、クリック**OK**をクリックして変更を保存します。

新しいインスペクション設定プロファイルを追加するには

1. Profilesビューで、Newをクリックします。
2. 開いたNew Profileウィンドウで、プロファイルの属性を編集します。
3. クリックOK。

セキュリティゲートウェイにインスペクション設定プロファイルを割り当てるには

1. Inspection Settings > Gatewaysビューで、セキュリティゲートウェイを選択し、Editをクリックします。
2. 表示されたウィンドウで、インスペクション設定プロファイルを選択します。
3. クリックOK。

インスペクション設定の例外を設定するには

1. Inspection Settings > Exceptionsビューで、Newをクリックして新しい例外を追加するか、例外を選択してEditをクリックして既存の例外を修正します。

   Exception Ruleウィンドウが開きます。
2. 例外の設定を行います。
   - Apply To- 例外を適用するProfileを選択
   - Protection- 設定を選択
   - Source- ソースNetwork Objectを選択するか、IP Addressを選択してソースIPアドレスを入力
   - Destination- 目的地を選択Service Object
   - Service- Port/Range、TCP、またはUDPを選択し、宛先ポート番号またはポート番号の範囲を入力
   - Install On- 例外をインストールするセキュリティゲートウェイを選択
3. クリックOK。

変更を強制するために、アクセスコントロールポリシーをインストールします。

SmartTasks

Management SmartTaskは、システム内のさまざまなトリガに応じた自動アクションを設定することができます。SmartTaskはトリガとアクションの組み合わせです。

- **トリガ**はイベントであり、現在はポリシーのインストールやセッションの公開など、既存の管理操作の観点から定義されています。
- **アクション**は、スクリプトの実行、Webリクエストの投稿、電子メールの送信など、トリガイベントの後に行われる自動的な応答です。

使用可能なトリガ

注 - SmartConsoleに表示される順番に並んでいます。

- **Before Publish** - 管理者がセッションを公開するときにトリガされます。SmartTaskは、セッションのメタデータ(公開管理者、ドメイン情報、セッション名) をアクションに渡します。ローカルのManagement APIサーバが利用可能な場合、公開しようとしているセッションの変更は、"show changes" APIへの応答としてフォーマットされます。
- **After Publish** - 管理者がセッションの公開を行った後にトリガされます。SmartTaskは、**Before Publish**トリガと同じ情報をアクションに渡します。
- **Before Install Policy**- ポリシーがインストールされる前に実行。SmartTask は、インストールするパッケージ、インストールを開始した管理者、タスクの結果など、ポリシーインストールタスクに関連するアクション情報を提供します。さらに、各セキュリティゲートウェイに現在インストールされているポリシーと、現在の操作でインストールが予定されているポリシーの詳細を提供します。
- **After Install Policy** - ポリシーがインストールされた後に実行。SmartTaskは、インストールされたパッケージ、インストールを開始した管理者、タスクの結果など、ポリシーのインストールタスクに関連する情報をアクションに渡します。
- **CloudGuard Controller Event**- SmartConsole >**Logging & Monitoring** view >**Logs** タブで、このクエリに一致する新しいログが生成されたときに発行されます:

  ```
  blade:"CloudGuard IaaS" AND severity:Critical
  ```

  詳細情報

  Management Serverは、このJSONフォーマットでイベントを作成します:

  ```
  {
      "severity": "<VALUE1>",
  ```

```
    "log-description": "<VALUE2>",
    "product": "CloudGuard IaaS",
    "gateway-name": "<VALUE3>",
    "datacenter-name": [
    "<VALUE4>",
    "<VALUE5>",
    "...",
    "<VALUEx>"
    ],
"version": "1.0"
}
```

これはスクリプトの例です(**Action**フィールドで**Run Script**を選択):

```
#!/bin/sh
input=$(echo $1 | base64 --decode)
severity=$(echo $input | jq '.severity')
message=$(echo $input | jq '."log-description"')
gw_name=$(echo $input | jq '."gateway-name"')
dc_name=$(echo $input | jq '."datacenter-name"')
echo -e "Subject: CloudGuard Controller event\r\n\r\nSeverity:
$severity\r\nMessage: $message\r\nData Center: $dc_
name\r\nGateway: $gw_name" | sendmail --domain=acme.com -f no-
reply@acme.com -v admin@acme.com --host=smtp.acme.com >
/dev/null
echo "Email sent"
```

- **After Submit**- 管理者が現在のセッションを別の管理者に承認してもらうために提出した後に発行される(*セッションの承認サイクル(SmartWorkflow および Identity Provider) (132ページ)*)。
- **Before Submit**- 管理者が現在のセッションを別の管理者に承認してもらうために提出する直前に発行される(*セッションの承認サイクル(SmartWorkflow および Identity Provider) (132ページ)*)。
- **Before Reject**- 管理者が送信されたセッションを拒否する直前に実行される(*セッションの承認サイクル(SmartWorkflow および Identity Provider) (132ページ)*)。
- **After Reject**- 管理者が送信されたセッションを拒否した後に実行されます(*セッションの承認サイクル(SmartWorkflow および Identity Provider) (132ページ)*)。
- **Before Login**- 管理者がSmartConsoleにログインする直前に実行。
- **After Approve**- 他の管理者が作成したセッションを管理者が承認した後に実行されます(*セッションの承認サイクル(SmartWorkflow および Identity Provider) (132ページ)*。

- **Before Approve**- 管理者が、他の管理者が作成したセッションを承認する直前に実行されます(*セッションの承認サイクル(SmartWorkflow および Identity Provider) (132ページ)*)。

利用可能なアクション

- **スクリプトの実行** - あらかじめ定義されたリポジトリスクリプトを実行します。スクリプトが取得する最初のパラメータは、トリガのデータを含むファイルへのパスです。スクリプトがローカルマシン上で実行されるように構成されていない場合、トリガのデータは、Base64エンコードされたJSONデータとして渡され、カスタムのビジネスロジックを実装するためにデコードすることができます。しかし、スクリプトがローカルマシンで実行されるように設定されている場合は、デコードの必要はありません。

  "Before"操作トリガで実行するように設定されたSmartTaskでは、リポジトリスクリプトは "result" とオプションの "message" フィールドを持つJSONオブジェクトを出力し、コード0で終了することにより、操作を中断するか継続するか知らせることができます。"result "フィールドの値が "failure "である場合、操作は中断されます。

  他のトリガで実行するように設定されたSmartTasksの場合、終了コード0は成功として扱われます。それ以外の終了コードは失敗として扱われます。

  注 - デフォルトでは、リポジトリスクリプトはローカルのSecurity Management Server上で実行されますが、Web APIを使用してカスタマイズすることができます。

- **Web Request** - 設定されたURLに対してHTTPS POST Webリクエストを実行します。トリガのデータは、リクエストのペイロードにJSONデータとして渡されます。

  注:
  - 設定するURLは、HTTPSで始まり、そのようなリクエストを処理できる対象Webサーバである必要があります。
  - 自己署名SSL証明書を持つWebサーバの場合、証明書のフィンガープリントを指定して信頼性を確立します。SmartTaskエディタで**Get Fingerprint**をクリックするか、Webブラウザで証明書を表示すると、フィンガープリントを取得できます。

  "Before"操作トリガで実行するように設定されたSmartTaskの場合、リポジトリスクリプトは、JSONオブジェクト "result"とオプションの "message" フィールドと200 OK というステータスで応答することにより、操作を中断するか継続するかを通知することができます。"result "フィールドの値が "failure "である場合、操作は中断されます。

  他のトリガで実行するように設定されたSmartTasksの場合、"200 OK" のリターンコードは成功として扱われます。それ以外の終了コードは失敗として扱われます。

- **Send Mail**- 設定されたEメールを送信します。

注

- このアクションを選択する前に、SMTPサーバを表す**タイプ**のServer**SMTP Server**オブジェクトを構成する必要があります。
- **Advanced**ペインでメールテンプレートを設定する必要があります。
- このアクションは以下のトリガにのみ使用できます: **After Install Policy After Submit**,**After Approve**,**After Publish**,**After Reject** 。

SmartTaskプロパティの設定

1. SmartTaskの一意の名前を入力します - nameプロパティは必須で、大文字と小文字を区別します。
2. トグルボタンでSmartTaskの**ON/OFF**を切り替えます。
3. オプション - SmartTaskの説明を入力します。
4. SmartTaskのトリガを選択します。
5. トリガが発生したときのアクションを選択します。
6. カスタムデータ - **カスタムデータ**フィールドにJSONオブジェクトを追加することで、トリガ情報と共に送信されるJSONデータに追加情報を追加できます。JSONカスタムデータは、トリガのペイロードに連結され、アクションに渡されます。
7. オプション - SmartTaskオブジェクトのタグを追加します。

SmartTaskの詳細プロパティ

利用可能な詳細オプションは、**General**タブで選択したアクションによって異なります。

Webリクエストの送信

- **タイムアウト** - リクエストがタイムアウトし、中止されるまでの秒数。
- **HTTPSリクエストがタイムアウトした場合** - タイムアウトをエラーとして扱い、イベントを中止するか、通常通り続行します。
- **X-chkp-shared-secret** - 対象のWebサーバがSecurity Management Serverを識別するために使用できる共有シークレットを入力します。この値はリクエストの一部として、発信Webリクエストの*X-chkp-shared-secret*ヘッダで送られます。

スクリプトの実行

- **タイムアウト** - リクエストがタイムアウトし、中止されるまでの秒数。
- **スクリプトの実行に失敗、またはタイムアウトした場合** - タイムアウト(または実行の失敗)をエラーとして扱い、イベントを中止するか、通常どおりに続行します。

メール送信

Eメールの詳細を入力:

- 対象
- Cc
- 送信者
- 件名
- 添付
- 本文

To"、"Cc"、"Sender "フィールドに定義済みのオプションを使用できるのは、SmartConsoleでメールアドレスを定義している管理者のみです。これらのフィールドは、IDプロバイダを介して接続されている管理者には使用できません。

SmartConsoleにメールアドレスが定義されていない管理者は、以下のいずれかを実行してください:

- 管理者の該当するメールアドレスを手動で入力。
- メールソフトで管理者のメーリングリストを作成し、該当フィールドにそのメーリングリストを使用。

例:

"**After Session Approve**" SmartTaskでは、管理者が提出者による変更をレビューし、承認します。

Email Configurationフィールドで:

"**To**"フィールドの代わりに、"**Submitter email**"フィールドに送信者全員のメーリングリストを入力します。

"**Cc**"フィールドの代わりに、"**All reviewers**"フィールドにすべてのレビュアーのメーリングリストを入力します。

"**Sender**"フィールドには、あらかじめ定義されている "**Reviewer email**" フィールドの代わりに、"SmartTask@mycompany.com" のようなダミーのEメールを入力します。

承認サイクルのワークフローの詳細については、以下を参照してください: *管理者向けセッションフロー (126ページ)*。

例

使用事例:

会社のポリシーで、データベースに変更を保存する前に、セッション名のプレフィックスとしてサービスリクエスト番号を付けて公開操作を使用するよう決められています。管理者はセキュリティポリシーを変更した根拠を確認することができます。

手順:

*Validate Session Name Prefix*を**Scripts Repository**に追加する。

1. リポジトリにスクリプトを保存します。

   手順

   a. **Gateways & Servers** >**Scripts** >**Scripts Repository** >**New** ()をクリック

   b. スクリプトに名前を付けます。

   c. **Content**のテキストボックスに、以下のスクリプトコードを貼り付けます。

   d. クリック**OK**してスクリプトをリポジトリに保存します。

Script Code

```
#!/bin/bash
JQ=${CPDIR}/jq/jq
data=`echo $1 | base64 --decode -i`

# Extracting the required session name prefix for the session
name based on the input JSON
sessionNamePrefix=`echo $data | $JQ -r  .\"custom-
data\".\"session-name-prefix\"`

# If there's no input session name prefix, publish is allowed
if [[ $sessionNamePrefix = "null" ]] || [[ -z
"$sessionNamePrefix" ]]; then
    printf '{"result":"success"}\n'
    exit 0
fi

# Extracting the actual session name
sessionName=`echo $data | $JQ -r .session.\"session-name\"`

# Abort the publish if the session doesn't contain a name at
all
if [[ $sessionName = "null" ]]; then
    m1="Corporate Policy requires you to use a service
request number for the session's name prefix."
    m2="For example: ${sessionNamePrefix}######"
    m3="Session name is missing. Please change your session's
name to meet the requirements and try to publish again."
    printf '{"result":"failure","message":"%s %s
 %s"}\n' "$m1" "$m2" "$m3"
    exit 0
fi
```

```
# Abort the publish if the session name doesn't match the
expected prefix
if [[ ! $sessionName == $sessionNamePrefix* ]]; then
    m1="Corporate Policy requires you to use a ticket number
as the session's name."
    m2="For example: ${sessionNamePrefix}###### "
    m2=${m2//\"/\\\"}
    m3="Please change your session's name to meet the
requirements and publish again."
    printf '{"result":"failure","message":"%s %s
 %s"}\n' "$m1" "$m2" "$m3"
    exit 0
else
    # Session name matches the expected prefix, publish is
allowed
    printf '{"result":"success"}\n'
    exit 0
fi
```

2. セッション検証スクリプトを実行するSmartTaskを作成します。

   手順

   a. 管理と設定 >**Tasks** > SmartTasks >**New** ()へ移動します。

   b. 新しいSmartTaskに名前を付けます("`Validate Session Name Before Publish`"と呼ぶことができます) 。

   c. **Trigger and Action**セクションで、ドロップダウンメニューから

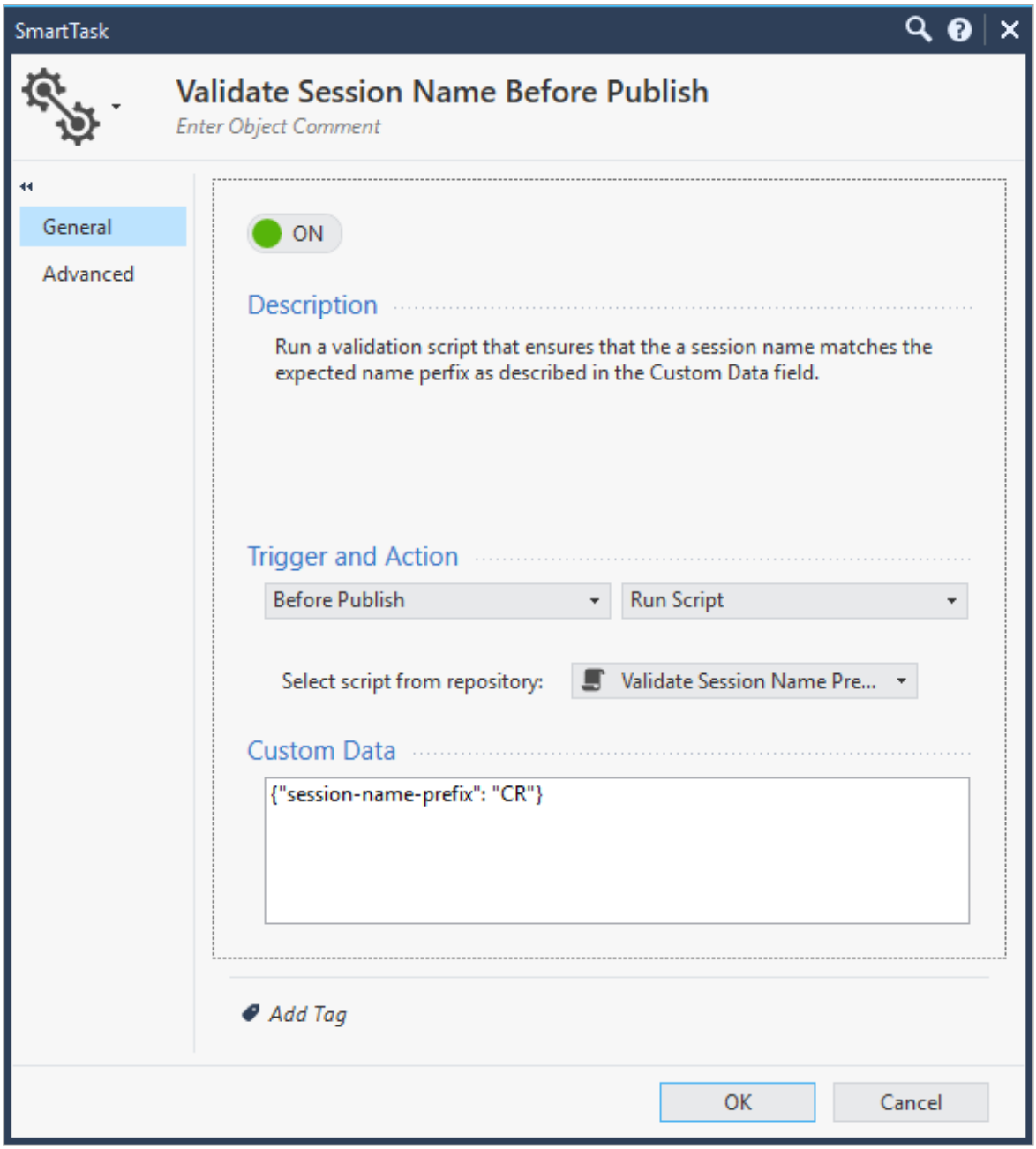
      Before PublishRun Script。

   d. **Select script from repository**ドロップダウンで、ステップ1で保存したスクリプトを選択します。

   e. **Custom Data**フィールドに、この文字列を入力します。

      {"session-name-prefix": "CR"}

      注 - 変数 "**session-name-prefix**"は、ステップ1のスクリプトの冒頭で使用された変数と関連しています。これらが同一でない場合、このスクリプトは動作せず、処理は失敗します。



3. SmartConsoleセッションを公開する。
4. ネットワークオブジェクトを追加します。
5. 必要なプレフィックスを使用して変更を公開します。

注 - プレフィックスを使用せずにセッションを公開すると、処理に失敗します。

IoTデバイス向けネットワークセキュリティ

重要 - R81.20 以降では、Infinity PortalのIoTネットワークセキュリティアプリケーションを使用してIoTポリシーを設定すると、SmartConsoleのIoT Policy Layerのすべてのオブジェクトが読み取り専用になります。これらのオブジェクトを編集するには、Infinity PortalのIoTネットワークセキュリティアプリケーションのみを使用します。

はじめに

病院、産業、スマートビルディングなど、現代の作業環境におけるIoTデバイスの使用は複雑で、その代償として、悪質で有害なサイバー攻撃にさらされています。IoTデバイスへの悪質なサイバー侵入は、多くの企業に多大な経済的損失をもたらしています。これらの攻撃は、金銭的損失や物理的被害に加え、データ漏洩や改ざん、ランサムウェア、さらにはサービス妨害につながる可能性があります。

攻撃を受けやすい一般的なIoTデバイス:

スマートビルディング/オフィス	ヘルスケア	業種
HVAC	HVAC	HVAC
プリンター、コピー機、ファクシミリ	プリンター、コピー機、ファクシミリ	プリンター、コピー機、ファクシミリ
エレベータ	エレベータ	エレベータ
監視カメラ	監視カメラ	監視カメラ
LANに接続された強化されていないキオスク端末	LANに接続された強化されていないキオスク端末	LANに接続された強化されていないキオスク端末
アクセス制御ポイント	アクセス制御ポイント	アクセス制御ポイント
プログラマブルロジックコントローラ(PLC)	プログラマブルロジックコントローラ(PLC)	プログラマブルロジックコントローラ(PLC)
サーモスタット	サーモスタット	サーモスタット
照明	照明	照明
家庭用スマートメーター	MRI装置	--
火災報知器	火災報知器	火災報知器

スマートビルディング/オフィス	ヘルスケア	業種
N/A	超音波装置	--
--	Cアーム	--
--	輸液ポンプ	--
--	血糖値測定器	--
--	患者用モニタ	--

IoTデバイスが脆弱性を持つ理由:

- 古いバージョンのソフトウェア、レガシーOS、またはOSなし
- 基本的なマイクロコントローラ
- セキュリティバイデザインがない
- デバイス管理の欠如
- シャドウデバイス
- 運用上の制限

Check PointのInfinity for IoTは、企業のITとIoTデバイス、スマートビルディングデバイス、産業用IoT、接続された医療機器に対して、包括的なネットワークセキュリティを提供します。

1. 様々なリソースからの複数の脅威指標を分析することで、IoTデバイスへの悪意ある意図や不正なアクセスを防止します。
2. 感染したデバイスが他のネットワーク要素に侵入することを防止します。
3. 内部ネットワークの細分化により、攻撃対象領域を最小限に抑えます。
4. IoTデバイスごとの詳細なインサイト情報を提供します。
5. IoTアセットを発見するために、サードパーティの検出エンジンを使用します。
6. 検出されたIoTデバイスの属性を用いて、個別のIoTポリシーレイヤーを作成します。

注

- Gaia Embeddedオペレーティングシステムを実行するCentrally Managed Quantum Sparkアプライアンスでは、アクセスコントロールポリシーにおけるIoTアセットの強制はサポートされていません。
- Check Pointは、Quantum IoT Protectというクラウドベースの IoTインスペクションサービスも提供しています。
  このサービスでは、ディスカバリを含め、すべてがCheck Pointのソフトウェアによって実行されます。
  詳細は*Quantum IoT Protect Administration Guide*。

事前準備

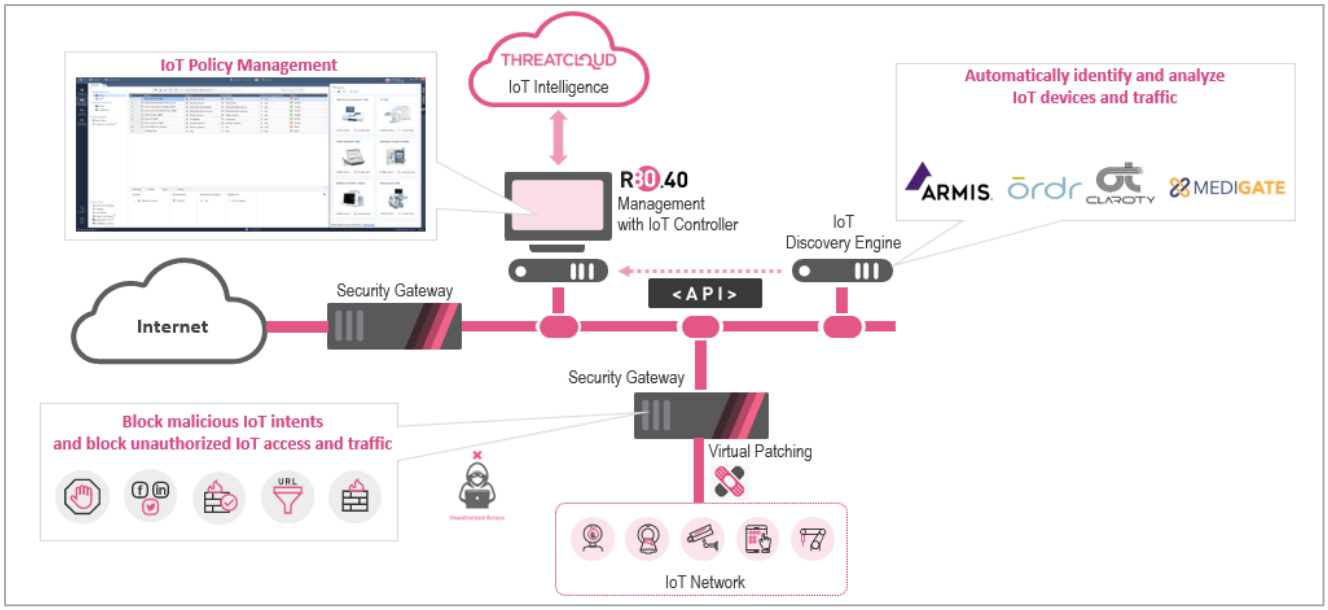
- Check Point認定のIoTサードパーティディスカバリサービスをネットワーク上にインストールし、管理サーバに接続します。
- ディスカバリーサービス
  - 産業/エンタープライズ:
    - Armis
    - Claroty
    - Indegy
    - Ordr
    - SAM
    - SCADAfence
  - 医療:
    - Medigate
    - CyberMDX
    - Cynerio
- Identity Awareness Web APIは、実施するセキュリティゲートウェイで有効になっている必要があります(設定は自動的に行われます)。
- Security GatewayバージョンR80.10以上

ネットワークの概要

Check PointのInfinity for IoTは、IoTベースのきめ細かいポリシーを適用することで、包括的なIoTサイバーセキュリティを実現します。Check PointのIoT保護ソリューションは、病院、産業、スマートビル、オフィスなどを集結させ、IoT攻撃を軽減、さらには排除することができます。

- IoTデバイスとトラフィックの特定と分析
- IoTポリシー実施ポイントの展開
- IoTの悪意ある意図の特定、ブロック

ネットワーク図



IoTサードパーティディスカバリーサービスの設定

Check Point Infinity for IoT で IoT デバイスを悪意のある攻撃から保護するには、IoT Third Party Discovery Service を設定する必要があります。IoT サードパーティ検出サービスは、Check Point の管理サーバと IoT サードパーティ検出エンジンとの接続を設定します。

IoT Third Party Discoveryエンジン:

- 接続されたIoTアセット(主に産業やヘルスケア分野)を検出します。
- 検出されたアセットをゾーンにグループ化します。
- 検出されたアセットと推奨されるポリシーをCheck Point Management Serverで共有します。

IoTサードパーティディスカバリーサービスを定義するには

ステップ	手順
1	SmartConsole > Manage & Settings > **Blades** > **IoT Third Party Discovery Service** > **Create Controller**へ移動します. **New IoT Third Party Discovery Service**ウィンドウが開きます。

ステップ	手順
2	設定するにはGeneral tab: a. Hostname、Port、Pre-shared Keyを入力します。事前共有鍵は、認証されたIoTサードパーティディスカバリーサービスによって提供され、IoTサードパーティディスカバリーサービスの認可および認証のために使用されなければなりません。 b. クリックOK. Certificate Trustウィンドウが開きます。確認の前に、証明書が有効であること、IoT Third Party Discovery Serviceが証明書の所有者であることを確認します。 Infinity for IoTは、Identity Awareness APIを利用しています。簡単に有効化するために、IoTの実施を行うゲートウェイを選択します。 Gatewaysタブを設定するには ■ IoTトラフィックの強制ゲートウェイを選択します。 Policiesタブを設定するには: a. IoT layerに適用するPolicyを選択します。 b. クリックOK。
3	SmartConsoleセッションを公開する。
4	ポリシーをインストールします。

新しいIoT Third Party Discovery Serviceを設定すると、選択したプロファイルに新しいIoTポリシーレイヤー、新しいThreat Preventionプロファイル、およびThreat Preventionポリシーの新しいルールが生成されます。

既存のIoTサードパーティディスカバリーサービスから新しいIoTサードパーティディスカバリーサービスを作成するには

1. SmartConsoleで、オブジェクトエクスプローラーペインに移動します。
2. 既存のIoTサードパーティディスカバリーサービスを右クリックし、Newを選択します。

ポリシーへのIoTアセットの追加

IoTポリシーを設定した後、IoTアセットを手動でポリシーに追加することができます。

ポリシーは3つのカテゴリに分かれます。

カテゴリ	説明
ユーザ定義	管理者が使用します。

カテゴリ	説明
自動生成	ネットワークトラフィックやIoTのネットワークパターンから生成されるルール。
クリーンアップ	検出された異常に対するルールセット。

IoTアクセスルールを定義するには

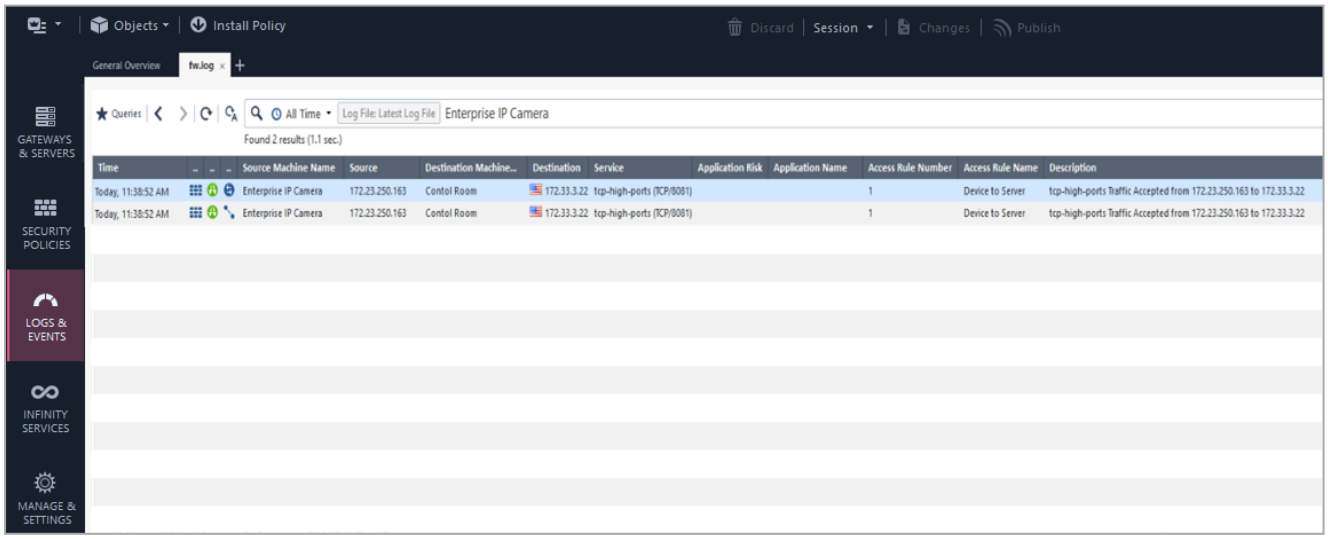
ステップ	手順
1	セキュリティポリシー > アクセスコントロールから、**IoT Layer**を選択します。
2	**User-Defined Section**をクリックし、プラス記号をクリックします。
3	**Source and/or Destination field**で、プラス記号 > **Add new item...**をクリックします。 **Add new item**ウィンドウが開きます。
4	**Import > IoT Controllers**を選択し、ルールに追加するIoTアセットを選択します。

IoTログのInfinity

Check PointのIoT Security Managerを使用することで、セキュリティチームは、製造元名、モデル、シリアル番号、設置場所などの詳細なIoTデバイス情報を確認することができます。完全なログを取ることで、デバイスの動作とイベント調査のためのフォレンジックを、より明確かつ文脈的に理解することができます。

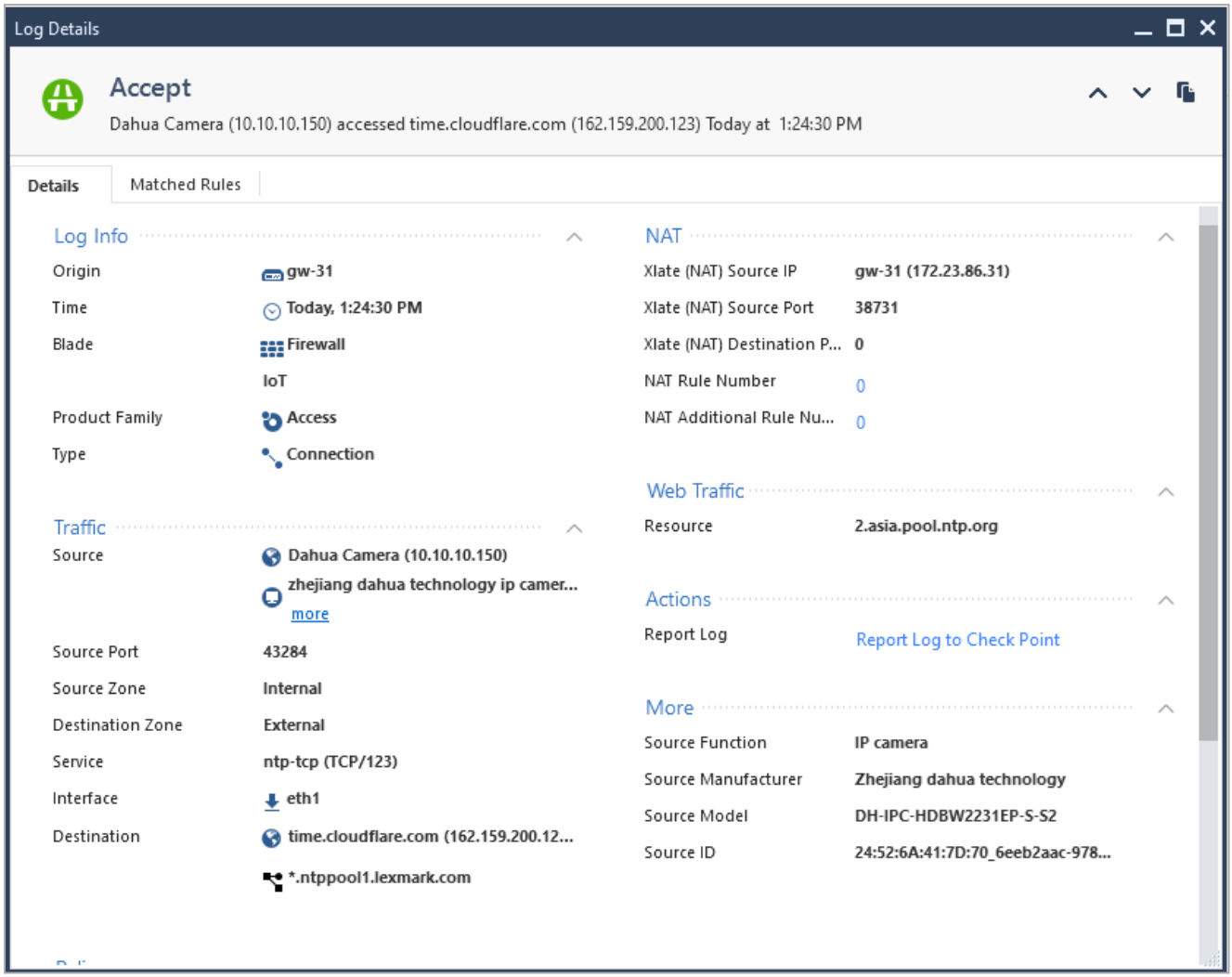
例1 - IoTアセット情報によるログ検索

ログのフィルタリングを簡素化するために、豊富なログデータを利用した高度なログ検索。



例2 - 拡張ログデータ

IoTログデータには、ログに含まれるIoTアセットを特定するのに役立つ豊富な情報が含まれています。



ハイアベイラビリティ(HA) 管 理

この章 では、Management High Availabilityの構 成 について説 明します。

ハイアベイラビリティ(HA) 管 理 の概 要

ハイアベイラビリティは、管 理 サーバの冗 長 化 とデータベースのバックアップです。同 期 されたサーバ は、同じポリシー、ルール、ユーザ定 義 、ネット ワークオブジェクト 、およびシステム構 成 設 定 を持ちま す。

管 理 ハイアベイラビリティは、組 み込 みのリビジョンテクノロジーを使 用し、ハイアベイラビリティ手 順 で 前 回 の同 期 以 降 に行 われた変 更 のみを同 期 させることができます。これにより、以 下 を実 現しま す。

- ピア管 理 サーバ間 のリアルタイム更 新 。
- 管 理 サーバリソースへの影 響 を最 小 限 に抑 えます。

最 初 にインスト ールされた管 理 サーバがプライマリになります。プライマリSecurity Management Serverに障 害 が発 生 した場 合 、またはメンテナンスのためにオフラインになった場 合 、管 理 者 はセカ ンダリサーバが引 き継 ぐように切 り替 えを開 始 することができます。

注 :

- セキュリティゲート ウェイのハイアベイラビリティ(および負 荷 分 散) 環 境 については、 以 下 を参 照 してください。*R82 ClusterXL Administration Guide*。
- エンド ポイント セキュリティのハイアベイラビリティ環 境 については、以 下 を参 照 してく ださい。*R82 Harmony Endpoint Security Server Administration Guide*。

ハイアベイラビリティ環境

Management High Availability環境には、以下のようなものがあります。

- アクティブSecurity Management Server 1台
- 1台以上のスタンバイSecurity Management Server

完全な冗長性を確保するため、アクティブ管理サーバは一定時間ごとにセカンダリサーバとデータベースを同期させます。

アクティブとスタンバイ

標準的なハイアベイラビリティ構成では、一度に1つのアクティブサーバが使用されます。管理者は、アクティブサーバを使用してハイアベイラビリティ設定を管理します。アクティブサーバは、定期的にスタンバイサーバと自動的に同期します。スタンバイサーバは、読み取り専用モードでのみ開くことができます。アクティブサーバに障害が発生した場合、スタンバイサーバをアクティブサーバにするためのチェンジオーバーを開始することができます。アクティブサーバとの通信に失敗する場合、アクティブサーバが複数台存在する可能性があります。これをコリジョンモードと呼びます。

プライマリサーバとセカンダリサーバの比較

管理サーバをインストールする順番で、プライマリかセカンダリかを定義します。最初にインストールされた管理サーバがプライマリアクティブサーバとなります。Security Management Serverをさらにインストールする場合は、セカンダリとして定義します。セカンダリサーバは、デフォルトではスタンバイサーバです。

Management High Availability環境でのバックアップと復元に関する重要事項:

- 一貫性した環境をバックアップおよび復元するには、ハイアベイラビリティ環境内のすべてのサーバから同時にバックアップとスナップショットを収集し、復元するようにしてください。
- バックアップ操作が完了するまで、他の管理者がSmartConsoleで変更を加えないよう注意してください。

詳細:

- GaiaバックアップとGaiaスナップショットについては次を参照: *R82 Gaia Administration Guide*。
- "`migrate export`"と"`migrate import`"コマンドについては次を参照: *R82 CLI Reference Guide*。
- `mds_backup`"と"`mds_restore`"コマンドについては次を参照: *R82 CLI Reference Guide*。
- Virtual Machine Snapshotsについては、ベンダーのドキュメントを参照してください。

SmartConsoleでのセカンダリSecurity Management Serverの設定

プライマリSecurity Management Serverに接続されたSmartConsoleで、セカンダリSecurity Management ServerのCheck Point Hostオブジェクトを作成します。SmartConsoleセッションを公開すると、プライマリSecurity Management Serverとセカンダリ Security Management Serverの間で同期が開始されます。

SmartConsoleでセカンダリSecurity Management Serverを設定するには

1. SmartConsoleでプライマリSecurity Management Serverにアクセスします。
2. **Object Explorer**で、**New > More > Network Object > Gateways and Servers > Check Point Host**をクリックします。
3. **General Properties**ページで、セカンダリSecurity Management Serverの一意の名前とIPアドレスを入力します。
4. **Software Blades**セクションで、**Management**タブを開き、**Network Policy Management**を選択します。

   これにより、**Secondary Server**、**Logging and Status**、**Provisioning**が自動的に選択されます。
5. セカンダリSecurity Management ServerとプライマリSecurity Management Serverの間にSICトラストを作成します:
   a. クリック**Communication**。
   b. セカンダリサーバのSICアクティベーションキーを入力します。
   c. クリック**Initialize**。
   d. クリック**Close**。
6. クリック**OK**。
7. SmartConsoleセッションを公開するセッションの変更をデータベースに保存します。

   Security Management Server間の初期化および同期が開始されます。
8. SmartConsoleのシステム情報エリアにあるタスクリストで、これらのタスクを監視します。タスクリストで完全な同期が完了したことが表示されるまで待ちます。
9. **High Availability Status**ウィンドウを開きアクティブSecurity Management Serverが1つ、スタンバイSecurity Management Serverが1つあることを確認します。
10. 各セキュリティゲートウェイ/クラスタについて、セキュリティゲートウェイ/クラスタオブジェクトを開き、[**Fetch Policy**]で[**Add**]をクリックし、セカンダリSecurity Management Serverを追加します。

注 - プライマリSecurity Management Serverに管理者を作成した場合、`cpconfig`、プライマリサーバからセカンダリサーバへの完全な同期が行われるまで、管理者はセカンダリSecurity Management ServerのSmartConsoleにログインできません。

アクティブサーバとスタンバイサーバの同 期

アクティブサーバとスタンバイサーバの同 期 、およびSmartConsoleセッションの公 開 は、一 定 時 間 ごとに行 われます。公 開 されていないセッションは同 期 されません。

ハイアベイラビリティのモニタ

High Availability Statusウィンドウには、ハイアベイラビリティ構 成 の各 Security Management Serverのステータスが表 示 されます。

ハイアベイラビリティ環 境 のサーバステータスを確 認 するには

1. SmartConsoleを起 動 し、プライマリサーバまたはセカンダリサーバに接 続 します。
2. **Menu**で、**High Availability**をクリックします。

High Availability Statusウィンドウが開きます。

ハイアベイラビリティの管 理 サーバとそのピアについては、**High Availability Status**ウィンドウが表 示 されます。

- 警 告 またはエラーメッセージ - このメッセージは、ハイアベイラビリティのピア間 に問 題 がある場 合 に表 示 されます。
- **Connected To**- SmartConsoleが接 続 されているサーバ。また、サーバのハイアベイラビリティモード(アクティブまたはスタンバイ) 、サーバの同 期 状 況 や動 作 も表 示 されます。
- **Peers**- 接 続 されているサーバが見 ているサーバ。また、各 サーバのハイアベイラビリティモード(アクティブまたはスタンバイ) 、各 サーバの同 期 状 況 やアクションも表 示 されます。

同 期 ステータスとアクションのモニタリング

ステータスメッセージは、システム全 体 に適 用 される一 般 的なものと、特 定 のアクティブサーバまたはスタンバイサーバに適 用 されるものがあります。一 般 的なメッセージは、黄 色 の概 要 バナーに表 示 されます。

概 要 バナーでの一 般 的なステータスメッセージ	説 明
	プライマリ Security Management Serverのデータベースは、セカンダリのデータベースと同じです。
一 部 のサーバが同 期 できませんでした。	通 信 の問 題 で同 期 できない、またはその他 の同 期 問 題 があります。
	アクティブサーバとスタンバイサーバが通 信 していません。
通 信 問 題	一 部 のサービスが停 止 している、またはアクセスできません。

概要バナーでの一般的なステータスメッセージ	説明
衝突またはHAコンフリクト	複数の管理サーバがアクティブに設定されています。2台のアクティブサーバは互いに同期できません。

指定されたアクティブ管理サーバに接続されている場合：

ステータスウィンドウ領域：	ピアステータス	追加情報
接続：	アクティブ	SmartConsoleはアクティブな管理サーバに接続されています。
ピア	スタンバイ	ピアはスタンバイ状態です。次のメッセージが表示されることもあります。 ■ 同期問題、前回同期 ■ 同期に成功。最終同期時間：<time> ■ 通信なし
	通信なし、最終同期時間	
	アクティブ	アクティブに定義された2つのサーバの間に衝突が存在します。

指定したスタンバイ管理サーバに接続した場合：

ステータスウィンドウ領域：	ピアステータス	説明
接続：	スタンバイ	最終同期時刻も表示されます。
ピア	アクティブ	ピアはスタンバイ中です。次のメッセージが表示されることもあります。 ■ 通信なし、最終同期時間 ■ OK、最終同期時刻：<time> ■ 同期問題、最終同期時間(任意の方向)
	スタンバイまたは不明	通信なしと表示される場合もあり。

サーバをアクティブまたはスタンバイに変更する

アクティブサーバは、定期的に、またセッションの公開時にも、スタンバイサーバと同期をとります。公開されていないセッションは同期されません。

プライマリ(アクティブ) とセカンダリ(スタンバイ) の管理サーバの切り替えは、自動的には行われません。アクティブに障害が発生した場合や、アクティブをスタンバイに変更する必要がある場合は、手動で変更する必要があります。管理サーバがスタンバイになると、読み取り専用になり、新しいアクティブサーバからすべての変更を取得します。

切り替えを開始すると、スタンバイがアクティブになった後、すべての公開データが新しいアクティブから新しいスタンバイサーバに同期されます。新アクティブのデータが新スタンバイのデータを上書きします。*未公開*の変更は同期されません。

ベストプラクティス - スタンバイSecurity Management Serverへの切り替えを開始する前に、SmartConsoleセッションを公開することをお勧めします。

アクティブとスタンバイを交換するには

1. SmartConsoleでSecurity Management Serverにアクセスします。
2. メニューボタンをクリックし、**High Availability**を選択します。

   High Availability Statusウィンドウが開きます。
3. **Action**ボタンを使って、スタンバイサーバをアクティブに変更します。

これにより、従来のアクティブサーバがスタンバイに変更されます。

コリジョンモードでの作業

複数のサーバをアクティブにすることができます。プライマリに接続できない場合は、これを実行する必要があるかもしれません。スタンバイをアクティブに変更すると、現在のアクティブサーバにスタンバイになるよう指示することなくアクティブになります。これは*コリジョンモード*として知られています。後でアクティブサーバの1つをスタンバイに変更し、標準の構成に戻すことができます。

コリジョンモードでは、アクティブサーバがネットワークに接続されていても、同期されません。どちらかをスタンバイに変更すると、同期が開始され、スタンバイサーバのデータが残りのアクティブのデータで上書きされます。

アクティブとスタンバイの切り替え

プライマリ(アクティブ) とセカンダリ(スタンバイ) の管理サーバの切り替えは、自動的には行われません。アクティブに障害が発生した場合や、アクティブをスタンバイに変更する必要がある場合は、手動で変更する必要があります。管理サーバがスタンバイになると、読み取り専用になり、新しいアクティブサーバからすべての変更を取得します。

ハイベイラビリティのトラブルシューティング

以下のエラーメッセージは、同期に失敗したときにHigh Availability Statusウィンドウに表示されます。

通信していません

解決策:

1. サーバ間の接続を確認します。
2. SICをテストします。

Collision or HA Conflict(衝突またはHAコンフリクト)

複数の管理サーバがアクティブに設定されています。

解決策:

1. SmartConsoleのメインメニューから、**Management High Availability**を選択します。

   High Availability Statusウィンドウが開きます。

2. **Actions**ボタンを使って、アクティブサーバの1つをスタンバイに設定します。

   警告 - このサーバがスタンバイになると、そのデータはすべてアクティブサーバに上書きされます。

Sync Error(同期エラー)

解決策:

手動で同期を行います。

Unlocking the Administrator(管理者のロック解除)

ハイアベイラビリティ環境では、スタンバイ管理サーバで管理者がロックされている場合、アクティブ管理サーバでは管理者はロックされておらず、ロックされているように表示されません。そのため、Active Management Server上の管理者を解除することはできません。

管理者のロックを解除するには

スタンバイ管理サーバでAPIコマンド`unlock-administrator`を使用します。詳細は*Check Point Management API Reference*。

Endpoint Securityのある環境

Endpoint Securityを備えた環境では、追加の手順と情報が必要です。

詳細：*ハイアベイラビリティ*[R82 Harmony Endpoint Security Server Administration Guide]。

ハイアベイラビリティのディザスターリカバリ

最初にインストールされる管理サーバはプライマリサーバで、それ以降にインストールされるサーバはすべてセカンダリサーバです。プライマリサーバは同期マスタとして機能します。プライマリサーバが停止すると、セカンダリがプライマリに昇格して最初の同期が完了するまで、セカンダリサーバはデータベースの同期を行うことができません。

プライマリ管理サーバが恒久的に利用できなくなった場合：

セカンダリ管理サーバをプライマリに昇格させ、元のプライマリサーバのIPアドレスで新しいプライマリサーバを作成します。

ステップ	方法
1	セカンダリ管理サーバをスタンバイからアクティブに変更します。

2	セカンダリ管理サーバをプライマリにプロモートします(古いプライマリ管理オブジェクトのインスタンスを削除し、データベースをインストールする必要はありません) 。
	開始する前に - プライマリサーバがオフラインであることを確認してください。
	a. セカンダリサーバをアクティブに設定します。
	b. 昇格させるセカンダリ管理サーバで、次を実行します。
	`#$FWDIR/bin/promote_util`
	`#cpstop`
	c. `$FWDIR/conf/mgha*`ファイルを削除します。現在のセカンダリ設定に関する情報が含まれています。これらのファイルは、Check Pointサービスを起動する際に再作成されます。
	d. 新しく昇格したサーバに`mgmtha`のライセンスがあることを確認します。
	注 - すべてのライセンスには、推進中のSecurity Management ServerのIPアドレスが必要です。
	e. 昇格したサーバで`cpstart`を実行します。
	f. SmartConsoleを開いて次を実行します。
	i. 古いプライマリ管理オブジェクトのインスタンスをすべて削除します。
	すべてのインスタンスを表示するには、オブジェクトを右クリックし、**Where Used**を選択します。
	注 - 古いプライマリ管理サーバを削除すると、それまでのライセンスはすべて失効します。
	ii. データベースをインストールします。

3	古いプライマリ管理サーバのIPで新しいセカンダリ管理サーバをインストールします。
4	SICをリセットし、新しいセカンダリ管理サーバにSICを作成します。

元の設定に戻す(元のプライマリ管理サーバに再度設定する) 場合 :

ステップ	方法
1	新しいセカンダリ管理サーバをスタンバイからアクティブに変更します。

2	新しいセカンダリ管理サーバをプライマリ管理サーバに変更します。
	セカンダリ管理サーバをプライマリにプロモートします(古いプライマリ管理オブジェクトのインスタンスを削除し、データベースをインストールする必要はありません) 。
	開始する前に - プライマリサーバがオフラインであることを確認します。
	a. セカンダリサーバをアクティブに設定します。
	b. 昇格させたセカンダリ管理サーバで、以下を実行します:
	`#$FWDIR/bin/promote_util`
	`#cpstop`
	c. `$FWDIR/conf/mgha*`ファイルを削除します。現在のセカンダリ設定に関する情報が含まれています。これらのファイルは、Check Pointサービスを起動する際に再作成されます。
	d. 新しく昇格したサーバに`mgmtha`のライセンスがあることを確認します。
	注 - すべてのライセンスには、推進中のSecurity Management ServerのIPアドレスが必要です。
	e. 昇格したサーバで`cpstart`を実行します。
	f. SmartConsoleを開いて次を実行します。
	i. 古いプライマリ管理オブジェクトのインスタンスをすべて削除します。
	すべてのインスタンスを表示するには、オブジェクトを右クリックし、**Where Used**を選択します。
	注 - 古いプライマリ管理サーバを削除すると、それまでのライセンスはすべて失効します。
	ii. データベースをインストールします。

3	古いプライマリ管理サーバのIPで新しいセカンダリ管理サーバをインストールします。
4	SICのリセットとセカンダリ管理サーバへのSICの作成

重要 - Check Point製品のライセンスは、IPアドレスにリンクされています。災害リカバリの終了時には、ライセンスがサーバに正しく割り当てられていることを確認する必要があります。

コンプライアンス

Check Point Compliance Blade は、Check Pointのセキュリティインフラストラクチャを継続的にモニタする動的なソリューションです。このブレードは、CCM(継続的コンプライアンスモニタリング) 技術を使用して、セキュリティゲートウェイ、Software Blades、ポリシー、設定を、規制基準とセキュリティのベストプラクティスの広範なデータベースに照らして検査します。ブレードは、セキュリティ上の問題を修正するための対応措置を提案します。

コンプライアンスブレードは、次の自動スキャンを実行します:

- デイリー - 1日1回の自動スキャンで、CLIまたはスクリプトによるゲートウェイおよびポリシー設定の変更を検出します。
- SmartConsoleの変更 - 管理者がセキュリティゲートウェイまたはポリシー設定に影響を与えるオブジェクトを変更したときに検出する自動スキャン(スキャンは、変更を公開した後に実行されます) 。

手動でスキャンを実行することもできます。

Security Management Serverでコンプライアンスブレードを有効にするには

1. SmartConsoleの[ゲートウェイ & サーバ]ビューで、[Security Management サーバ]オブジェクトをダブルクリックします。

   Security Management Serverエディタが開きます。

2. **General Properties**ページで、**Management**に進み、コンプライアンスを選択します。
3. **OK**をクリックします。

コンプライアンスダッシュボードを表示するには

1. SmartConsoleのログ & イベントビューで、**+** をクリックして新しいタブを開きます。

   New Tabが開きます。

2. **Compliance**をクリックします。

コンプライアンス ビュー

コンプライアンスビューには5つのウィジェットがあります:

- Security Best Practices
- Gateways
- Blades

- Action Items and Messages
- Regulatory Compliance

コンプライアンススコアリングシステム

コンプライアンスブレードは、組織のセキュリティゲートウェイ、Software Blades、および規制に関する各ベストプラクティステストのスコアを数値で算出します。スコアは、検査された各オブジェクトの検査結果の平均です。

これは、Check Point Compliance Blade の採点システムです:

セキュリティステータス	スコア (%)	コメント
Poor	0-50	0 = 非準拠
中	50-75	
Good	75-99	
Secure	100	準拠
N/A	該当なし	以下の場合に表示: ■ 該当するSoftware BladeがSecurity Management Serverにインストールされていません。 または ■ セキュリティゲートウェイは検査機能をサポートしていません。

この章では、各コンプライアンスビューの操作方法について説明します。システム要件、トラブルシューティング、デバッグの詳細については、次を参照してください。sk120256.

セキュリティベストプラクティスコンプライアンス ビュー

セキュリティベストプラクティスのコンプライアンス ビューには、各 ベストプラクティスのステータス情 報 が表 示されます。

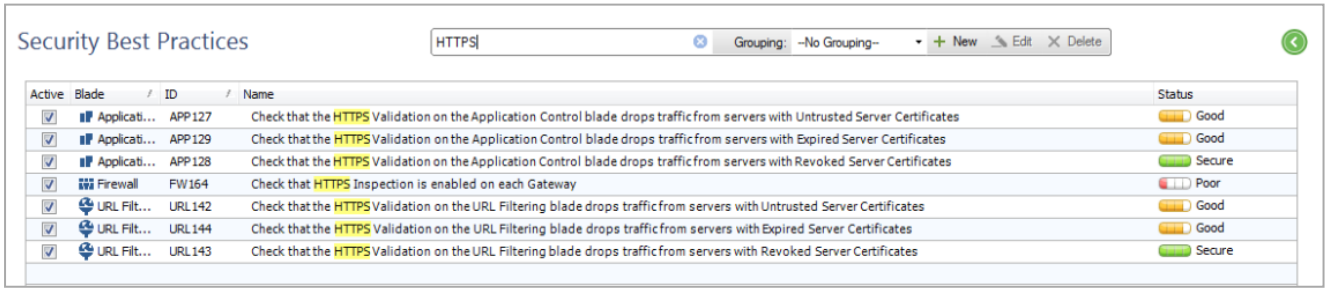
上 の表 は、ベストプラクティスに関 連 するこれらの詳 細 です:

- **Active**- ベストプラクティステストを選 択して有 効にする。クリアして無 効にする。
- **Blade**- このベストプラクティスに関 連 するブレード。
- **ID**- ベストプラクティスに割り当 てられたCheck Pointコンプライアンス ID。
- **Name**- ベストプラクティスに関 連 する規 制 要 件 の名 称 と簡 単 な説 明 。
- **Status**- 「Poor」「Medium」「Good」「Secure」「N/A」。「Poor」ステータスの項 目 は直 ちに解 決 することをお勧 めします。

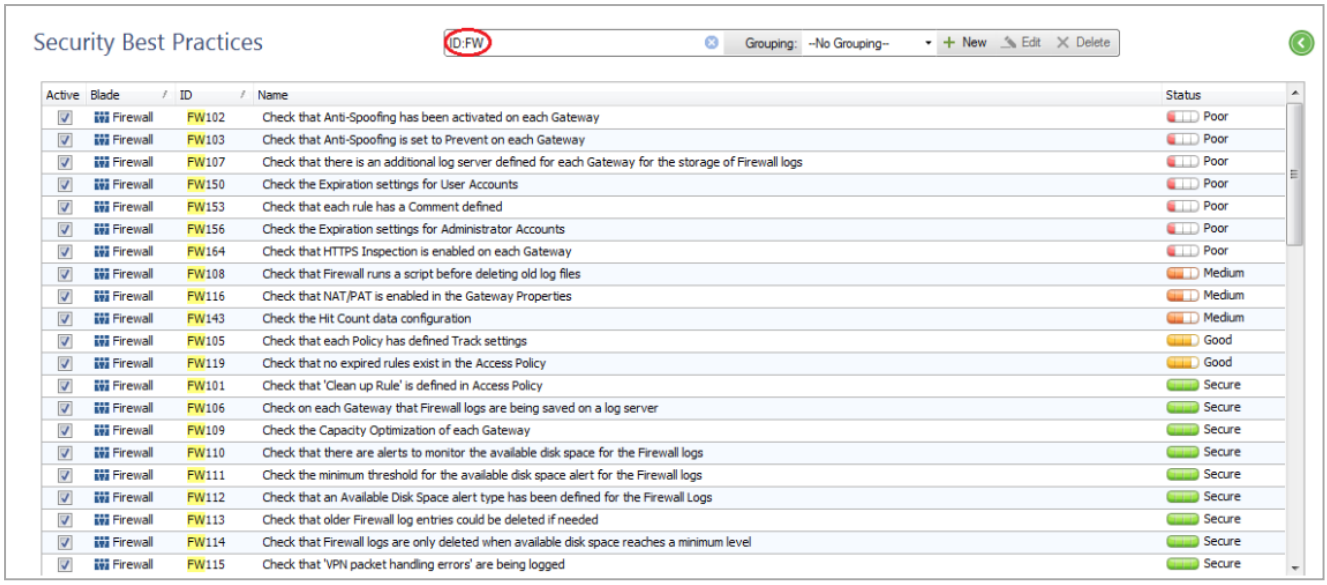
一 番 下 のセクションは、選 択したベストプラクティステストのこれらの項 目 を示 しています:

- **Description**- ベストプラクティステストの詳 細
- **Action Item**- 代 替 シナリオを含 む、準 拠に必 要 なステップ。
- **Dependency**- 選 択したベストプラクティスが他 のベストプラクティスに依 存 している場 合 に表 示される。このテストは、他 のベストプラクティスが適 合 している場 合 にのみ実 施 される。
- **Relevant Objects**- 選 択されたベストプラクティステストに関 連 するオブジェクトとそのステータス。選 択したベストプラクティスのテストを、指 定 したオブジェクトに対 して有 効 化 または無 効 化 することができる(このセクションは、ベストプラクティスが特 定 のオブジェクトにアプリケーションされる場 合 にのみ表 示) 。
- **Relevant Regulatory Requirements**- ベストプラクティスに適 用 されるすべての規 制 基 準 のリストへのリンク。

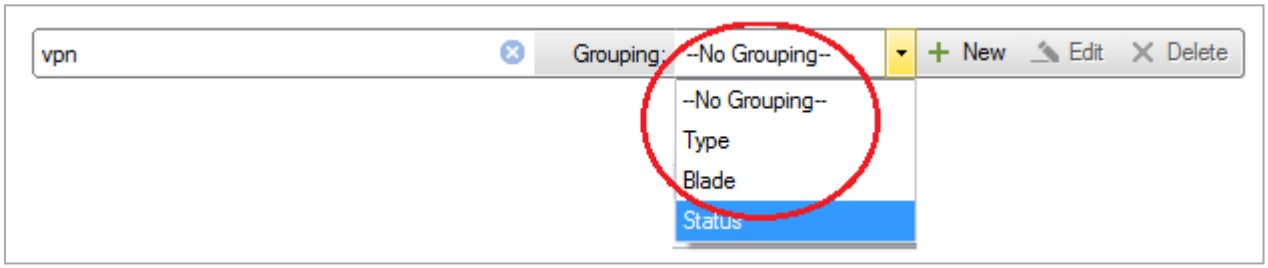
特 定 の値 を検 索 するには、検 索 ボックスに文 字 列 を入 力します:



特 定 のフィールドで特 定 のパラメータを検 索 するには、*field name:string*と入 力します。



結果をグループ化するには、グループ化フィールドで**Blade**または**Status**を選択します;



検索結果を特定のフィールドでソートするには、フィールドのヘッダをクリックします。

ユーザ定義のベストプラクティスの作成

組織のセキュリティ要件に基づいて、独自のカスタムセキュリティベストプラクティスを定義できます。

新しいファイアウォールセキュリティベストプラクティスを作成する:

1. **Compliance**タブ > **Security Best Practices**ペイン > **See All**をクリックします。
2. **New**をクリックし、**Firewall Best Practice**を選択します。

   New Firewall Best Practiceウィンドウが開きます。
3. このベストプラクティスに対して**Name**と**Description**を入力します。
4. このベストプラクティスで生成された**Action Item**を入力します。
5. **Best Practice Rule Definition**セクションで、表のセルにルールのマッチング条件を入力します。セキュリティベストプラクティスの一致は、すべてのテーブルセルがルールベース内の1つ以上のルールに一致する場合に発生します(論理AND)。

a. **Hit Count**- ヒット数のレベルを選択します。マッチは、ルールのヒットカウントが、指定されたヒットカウントレベルと等しいか、それを超えたときに発生します。例えば未使用のルールをルールベースで確認するには、**Hit Count Zero** を選択します。

b. **Name**

c. **Source**- 1つまたは複数のソースオブジェクトを選択します。

d. **Destination**- 1つ以上の宛先オブジェクトを選択します。

e. **VPN**- 1つまたは複数のVPNコミュニティを選択します。

f. **Services & Applications**- 1つまたは複数のサービスまたはアプリケーションを選択します。

g. **Action**- ルールがトリガするアクション。

h. **Track**- ルールの追跡方法。

i. **Install On**- ルールが適用されるセキュリティゲートウェイ/セキュリティクラスタ。

j. **Time**- ルールを適用する時間帯を選択します。

k. **Comment**- 必要に応じてコメントを入力します。

l. オプション: **Advanced Settings**をクリックして、スキャンするルールベースのパーセンテージとスキャンの方向 (**Top**または**Bottom**) を選択します。例えば、**Bottom 30%**を選択すると、ルールベースの30%を一番下 (ルールベースの最後のルール) からスキャンします。

注 - セルを右クリックし、**Negate Cell**を選択すると、そのセルをマッチングから除外できます。この機能は**Name** と**Comment** セルでは利用できません。

6. **Best Practice Scoring**セクションで次の設定を行います:

a. **Violation Definition**- ベストプラクティスがルールにマッチしたときにマッチするかどうかを定義します。いずれかのオプションを選択します。

- ルールが見つかった - ベストプラクティスがルールベース内のルールとマッチすると、一致となります。
- ルールが見つからない - ベストプラクティスがルールベース内のルールと一致しない場合に発生します。

Toleranceのレベルを選択する - 指定された数以上のマッチがあると違反が発生します(デフォルト = 0) 。例えば、許容範囲が0に設定されている場合、コンプライアンスブレードは最初の一致が発生した時点で違反を作成します。許容範囲が3に設定されている場合、コンプライアンスブレードは4番目の一致が発生した時点で違反を作成します。**Tolerance**オプションは**Rule found**オプションにのみ適用されます。

b. **Rule Index Display Criteria**- **Rule Index**ビューの**Relevant Objects**ペインに**Security Best Practices** (ルール番号) が表示されるタイミングを定義します。これにより、どのルールが違反の原因となっているのか、あるいは違反を防いでいるのかを簡単に確認することができます:

- **Display rules that match**- セキュリティベストプラクティスで指定された条件に一致するルールを表示します。
- **Display rules that don't match**- セキュリティベストプラクティスで指定された基準に一致しないルールを表示します。
- **Don't display rules**- ルールを表示しません。

7. **OK**をクリックします。

   新しいベストプラクティスがベストプラクティスのリストに追加されます。

8. 変更を公開します。

新しいGaia OSセキュリティベストプラクティスを作成します:

1. **Compliance**タブ > **Security Best Practices**ペイン > **See All**をクリックします。
2. **New**をクリックし、**Gaia OS Best Practice**を選択します。

   新しいウィンドウ(**Gaia OS Best Practice**) が開きます。

3. このベストプラクティスについて**Name**、**Description**を入力します。
4. このベストプラクティスによって生成された**Action Item**を入力します。
5. セキュリティゲートウェイで実行する**Practice Script**を入力するか、ファイルからスクリプトを読み込みます。
6. **Expected Output**スクリプトの出力が期待される出力と同じであれば、ベストプラクティスのステータスは安全です。
7. **OK**をクリックします。

   新しいベストプラクティスがベストプラクティスのリストに追加されます。

8. 変更を公開します。

ベストプラクティス - 新しいセキュリティベストプラクティスを作成したら、手動スキャンを実行することをお勧めします。スキャンは、設定の変更を反映するために、コンプライアンスステータスを再評価します。手動スキャンを行うには、「Manage & Settings」ビュー >**Blades** >「コンプライアンス」 >**Settings** >「**Rescan** 」ボタンをクリックします。スキャンの実行中は、[コンプライアンス] タブでアクションを実行できません。

ベストプラクティステストの有効化と無効化

テスト別、セキュリティゲートウェイ別、Software Blade別、またはその他のオブジェクト別に、ベストプラクティスの実施を有効化または無効化できます。アクティベーションの変更は、次回のスキャン後に適用されます。

デフォルトでは、すべてのベストプラクティステストがアクティブになっています。

組織全体のベストプラクティスを無効にするには

1. **Security Best Practices**ビュー > にアクセスし、ベストプラクティスを選択します。
2. 右クリックして、**Deactivate**を選択します。

   Expiration Detailsウィンドウが開きます。
3. **Never**を選択するか、有効期限を入力します。有効期限を選択した場合、ベストプラクティステストはその日に自動的に有効になります。
4. **Comment**ボックスに、このコンプライアンステストを無効化する理由を説明します。

現在アクティブでないベストプラクティステストをアクティブにするには

- **Security Best Practices**ビューに移動し、ベストプラクティスを選択し、右クリックして**Activate**を選択します。

  または
- 管理 & 設定 > 表示 >**Blades** > コンプライアンス >**Inactive Objects** >**Inactive Security Best Practices** > 該当するセキュリティベストプラクティスを選択し、**Remove** をクリックします。

特定のセキュリティゲートウェイのベストプラクティスを無効にするには

1. 管理と設定 > 表示 >**Blades** > コンプライアンス >**Inactive Objects**へ移動します。
2. **Inactive Gateways**セクションで、**Add**をクリックします。
3. セキュリティゲートウェイまたはセキュリティクラスタを入力または選択します。

注 - セキュリティゲートウェイのベストプラクティスを有効にするには、セキュリティゲートウェイを選択し、**Remove**をクリックします。プロンプトが表示されたら、**Yes**をクリックします。

特定のオブジェクトのベストプラクティスを無効にするには

1. 管理と設定 > 表示 >**Blades** > コンプライアンス >**Inactive Security Best Practices on Specific Objects**へ移動します。
2. **Inactive Gateways**セクションで、**Add**をクリックします。
3. セキュリティゲートウェイまたはセキュリティクラスタを入力または選択します。

ベストプラクティス - ベストプラクティステストを有効化または無効化した後、手動スキャンを実行することをお勧めします。スキャンは、設定の変更を反映するために、コンプライアンスステータスを再評価します。手動スキャンを行うには、Manage & Settingsビュー >**Blades** > コンプライアンス >**Settings** >**Rescan** ボタンをクリックします。スキャンの実行中は、[コンプライアンス] タブでアクションを実行できません。

ゲートウェイビュー

このウィジェットには、セキュリティゲートウェイのセキュリティステータスが表示されます。コンプライアンススコアが最も高い5つのセキュリティゲートウェイ、最も低い5つのセキュリティゲートウェイ、または事前に定義されたお気に入りのセットが表示されます。すべてのセキュリティゲートウェイの結果を見るにはSee All

特定のセキュリティゲートウェイ/セキュリティクラスタに適用されるベストプラクティスを表示するには、特定のセキュリティゲートウェイ/セキュリティクラスタをクリックします。

上の表は、ベストプラクティスに関連するこれらの詳細です:

- Active- ベストプラクティステストを選択して有効にする。クリアして無効にする。
- Blade- このベストプラクティスに関連するブレード。
- ID- ベストプラクティスに割り当てられたCheck Pointコンプライアンス ID。
- Name- ベストプラクティスに関連する規制要件の名称と簡単な説明。
- Status-「Poor」「Medium」「Good」「Secure」「N/A」。「Poor」ステータスの項目は直ちに解決することをお勧めします。

一番下のセクションは、選択したベストプラクティステストのこれらの項目を示しています:

- Description- ベストプラクティステストの詳細
- Action Item- 代替シナリオを含む、準拠に必要なステップ。
- Dependency- 選択したベストプラクティスが他のベストプラクティスに依存している場合に表示される。このテストは、他のベストプラクティスが適合している場合にのみ実施される。
- Relevant Objects- 選択されたベストプラクティステストに関連するオブジェクトとそのステータス。選択したベストプラクティスのテストを、指定したオブジェクトに対して有効化または無効化することができる(このセクションは、ベストプラクティスが特定のオブジェクトにアプリケーションされる場合にのみ表示) 。
- Relevant Regulatory Requirements- ベストプラクティスに適用されるすべての規制基準のリストへのリンク。

ブレード ビュー

このウィジェットには、Software Blades別のセキュリティステータスが表示されます。セキュリティのベストプラクティスが最も多く実装されている5つのSoftware Bladesの平均スコアが表示されます。特定のSoftware Bladeの結果を見るには、そのブレードをクリックします。すべてのSoftware Bladesの結果を見るにはSee All

上の表は、ベストプラクティスに関連するこれらの詳細です:

- Active- ベストプラクティステストを選択して有効にする。クリアして無効にする。
- Blade- このベストプラクティスに関連するブレード。
- ID- ベストプラクティスに割り当てられたCheck Pointコンプライアンス ID。
- Name- ベストプラクティスに関連する規制要件の名称と簡単な説明。
- Status-「Poor」「Medium」「Good」「Secure」「N/A」。「Poor」ステータスの項目は直ちに解決することをお勧めします。

一番下のセクションは、選択したベストプラクティステストのこれらの項目を示しています:

- Description- ベストプラクティステストの詳細
- Action Item- 代替シナリオを含む、準拠に必要なステップ。
- Dependency- 選択したベストプラクティスが他のベストプラクティスに依存している場合に表示される。このテストは、他のベストプラクティスが適合している場合にのみ実施される。
- Relevant Objects- 選択されたベストプラクティステストに関連するオブジェクトとそのステータス。選択したベストプラクティスのテストを、指定したオブジェクトに対して有効化または無効化することができる(このセクションは、ベストプラクティスが特定のオブジェクトにアプリケーションされる場合にのみ表示) 。
- Relevant Regulatory Requirements- ベストプラクティスに適用されるすべての規制基準のリストへのリンク。

アクションアイテムとメッセージビュー

ベストプラクティステストで不備が検出されると、Check Pointコンプライアンスブレードは自動的にアクションアイテムを生成します。アクションアイテムは、欠陥を修正するために取るべき是正措置の有用な説明を示しています。アクションアイテムに期日を割り当て、修正ステップをモニタリングすることができます。アクションアイテムが生成されるとき、期限は割り当てられません。修正手順を完了すると、Check Pointコンプライアンスブレードは次回のスキャン後にアクションアイテムを削除します。

このウィジェットには3つのセクションがあります:

- **アクションアイテム**

  このウィジェットは、組織の保留中のアクションアイテムの更新ステータスを表示します:

  - **Upcoming items**- 期限が今後30日以内のアクションアイテム。
  - **Future items**- 期日が30日以上経過したアクションアイテム。
  - **Unscheduled items**- 期限を定めていないアクションアイテム。
  - **Overdue items**- 期限を過ぎたアクションアイテム。

    ベストプラクティス - 期限を過ぎたアクションアイテムは直ちに解決します

  ステータスカテゴリのアクションアイテムを開くには、**Action Items**をクリックします:

  上の表で、アクションアイテムに関連するこれらの詳細をご覧ください:

  - **Due Date**- このアクションアイテムを解決する期日を指定します(オプション)。アクションアイテムが生成される際、期日は自動的に割り当てられません。
  - **Blade**- アプリケーションされるベストプラクティスに関連するブレード。
  - **ID**- 該当するベストプラクティスに割り当てられたCheck Pointコンプライアンス ID。
  - **Name**- アプリケーションされるベストプラクティスに関連する規制要件の名称と簡単な説明。
  - **Status**-「Poor」、「Medium」、「Good」、「Secure」、または「N/A」。「Poor」ステータスの項目は直ちに解決することをお勧めします。

  一番下のセクションには、選択したアクションアイテムの項目が表示されます:

  - **Action Item Description**- 準拠させるために必要なステップ。
  - **Due Date**- このアクションアイテムを解決する期日を指定します(オプション)。

- **Dependency**- 選択したベストプラクティスが他のベストプラクティスに依存している場合に表示されます。このテストは、他のベストプラクティスが適合している場合にのみ実施されます。
- **Relevant Objects**- 選択されたベストプラクティステストに関連するオブジェクトとそのステータス。選択したベストプラクティスのテストを、指定したオブジェクトに対して有効化または無効化することができます(このセクションは、ベストプラクティスが特定のオブジェクトにアプリケーションされる場合にのみ表示されます) 。
- **Relevant Regulatory Requirements**- ベストプラクティスに適用されるすべての規制基準のリストへのリンク。

■ **アラートメッセージ**

アラートは、設定の変更によってコンプライアンスステータスが低下した場合に生成されます。すべてのアラートメッセージを表示するには、**Security Alerts**をクリックします。

■ **システムメッセージ**

システムメッセージは、コンプライアンスパッケージの更新など、コンプライアンスに関連するシステムの問題を通知します。すべてのシステムメッセージを表示するには、**System Messages**をクリックします。

アクションアイテムに期日を割り当てるには

1. SmartConsoleで、ログ＆イベントビュー > コンプライアンスタブ >**Action Items and Messages** >**Pending Action Items** >**Unscheduled items** を開きます。
2. アクションアイテムを選択します。
3. **Action Item Description**セクションで、**Schedule Now**をクリックします。アクションアイテムにすでに期日が設定されている場合は、期日リンクをクリックして期日を変更します。
4. 開いたウィンドウで期日を入力または選択し、**OK**をクリックします。

規制コンプライアンスビュー

このウィジェットは、選択した規制基準のコンプライアンス統計を表示します:

- 各規制基準について検討された規制要件の数。
- コンプライアンスの平均点。

表示される規制基準を選択するには

1.  ペインの右上にあるこのアイコンRegulatory Complianceをクリックします。
2. Select Regulations and Standardsウィンドウで、Overviewに表示するスタンダードを選択します。

すべての規制要件のコンプライアンススコアを見るには、See Allをクリックします。

特定の規格の詳細を見るには、その規格をクリックします。上の表はこれらの項目を示しています:

- ID- ベストプラクティスに割り当てられたCheck PointコンプライアンスID。
- Status-「Poor」、「Medium」、「Good」、「Secure」、または「N/A」。「Poor」ステータスの項目は直ちに解決することをお勧めします。
- Name- 規制要件の名称と簡単な説明

下のセクションは、これらの項目を示しています:

- Description- ベストプラクティステストの詳細
- Relevant best practices- 選択した要件に適用可能なベストプラクティス、およびそのコンプライアンス状況。
- Relevant objects- 選択されたベストプラクティステストに関連するオブジェクトとそのステータス。選択したベストプラクティスのテストを、指定したオブジェクトに対して有効化または無効化することができます(このセクションは、ベストプラクティスが特定のオブジェクトにアプリケーションされる場合にのみ表示されます) 。

組織に適用される規制基準を選択できます。デフォルトでは、サポートされているすべての規制基準がアクティブになっています。

規制基準を有効または無効にするには

1. Manage & Settingsビュー > Blades > Compliance > Settingsに進みます。

   Settingsウィンドウが開きます。
2. Active Regulationsセクションで、該当する規制基準を選択/クリアします。
3. 変更を公開します。

SmartConsoleに規制基準をインポートするには

1. 適用される規制基準をXMLファイルでローカルに保存します。
2. **Manage & Settings**ビュー > **Blades** > **Compliance** > **Settings**に進みます。

   Settingsウィンドウが開きます。
3. **Active Regulations**セクションに行き、**Actions** > **Import**をクリックします。
4. インポートするXMLファイルを参照し、**Open**をクリックします。

   このレギュレーションは現在、**User-defined Regulations**のリストに表示されています。
5. 規定をダブルクリックします。

   規定ウィンドウが開きます。
6. **Save**をクリックします。

   完了までに数分かかる場合があります。
7. 変更を公開します。

ベストプラクティス - 規制基準リストに変更を加えた後、手動スキャンを実行することをお勧めします。スキャンは、設定の変更を反映するために、コンプライアンスステータスを再評価します。手動スキャンを行うには、**Rescan**セクションの**Engine Status**ボタンをクリックします。スキャンの実行中は、[コンプライアンス] タブでアクションを実行できません。

レポートの作成

コンプライアンス状況の概要や、特定の規制基準の実施に関するレポートを作成することができます。

レポートを作成するには

1. SmartConsoleのログ＆イベントビューで、+をクリックしてNew Tabを開きます。

   New Tabが開きます。

2. Reportsビューを選択します。
3. 表示されたリストからCompliance Bladeを選択します。
4. Openをクリックします。

   レポートが開きます。

5. オプション：ツールバーのActionsで、PDFとCSV形式でレポートを作成できます。エクスポートされたレポートを見つけるには、ログ＆イベントビュー > New Tab > Archiveを開きます。

規定に従ってレポートを作成するには

1. コンプライアンスビューで、Regulatory Compliancesペインに移動し、See Allを選択します。
2. 必要な規制基準をクリックします。
3. 上部のツールバーで、Generate Reportをクリックします。
4. 上部のツールバーから、これらの出力形式でレポートを作成することを選択できます：
   - PDFドキュメント
   - PDFを添付したEメール
   - プリンターへの出力
   - ブラウザへのHTML出力。

ICA管理ツール

メニュー

ICA管理ツールでは、管理者は次のことができます:

- 証明書の管理

  警告 - ICA管理ツールを使用して、SIC証明書またはVPN証明書を変更**しないで**ください。SmartConsoleのみで、SICおよびVPN証明書を変更します。ICA管理ツールは、証明書の作成など、ユーザ証明書の操作のみに使用します。

- CRLの再作成
- 内部認証局(ICA)パラメータの設定
- 期限切れの証明書の削除

注 - ICA管理ツールは、TLSをサポートしています。

Check Point ICAは、証明書とCRLの両方においてX.509標準に完全に準拠しています。詳細は、関連するX.509とPKIのドキュメント、およびRFC 2459を参照してください。

詳細:sk102837: Best Practices - ICA Management Tool configuration

ICA管理ツールへの接続

ICA管理ツールは、デフォルトでは無効になっています。

ICA管理ツールに接続するには

1. SmartConsoleで、必要な管理者オブジェクトとユーザオブジェクトを設定します。

   これらの管理者とユーザのために証明書を作成する必要があります。

   この証明書を使用して、ICA管理ツールおよびクライアントのWebブラウザで許可ユーザを設定します。

2. 管理サーバのコマンドラインで、ICA管理ツールの使用を許可する管理者とユーザを追加します。

   ```
   cpca_client set_mgmt_tool add ...
   ```

   参照:*cpca_client set_mgmt_tool (735ページ)*。

3. 管理サーバのコマンドラインで、ICA管理ツールを起動します。

```
cpca_client set_mgmt_tool on
```

参照: *cpca_client set_mgmt_tool (735ページ)*。

4. ICA管理ツールのステータスを確認します:

```
cpca_client set_mgmt_tool print
```

参照: *cpca_client set_mgmt_tool (735ページ)*。

5. 管理者/ユーザの証明書をWindows証明書ストアにインポートします:

   a. 必要な管理者 / ユーザを作成した際に保存した *.p12 ファイルを右クリックし、**Install PFX**をクリックします。

      Certificate Import Wizardが開きます。

   b. **Store Location**セクションで、該当するオプションを選択します:

      - **Current User**(これはデフォルトです)
      - **Local Machine**

   c. クリック**Next**。

   d. 必要な管理者/ユーザ証明書を作成したときに使用したのと同じ証明書パスワードを入力します。

   e. **Enable strong private key protection**をクリアします。

   f. **Mark this key as exportable**を選択します。

   g. クリック**Next**。

   h. **Place all certificates in the following store**を選択 > **Browse**をクリック > **Personal**を選択 > **OK**をクリックします。

   i. クリック**Next**。

   j. クリック**Finish**。

6. WebブラウザでICA管理ツールに接続します:

```
https://<IP Address of the Management Server>:18265
```

重要 - TCPポート18265が開いていることは脆弱性ではありません。ICA管理ツールポータルはSSLで保護されています。さらに、証明書を使用してアクセスできるのは、権限を与えられた管理者とユーザのみです。

7. このようなメッセージのダイアログボックスが表示されます:

```
Client Authentication

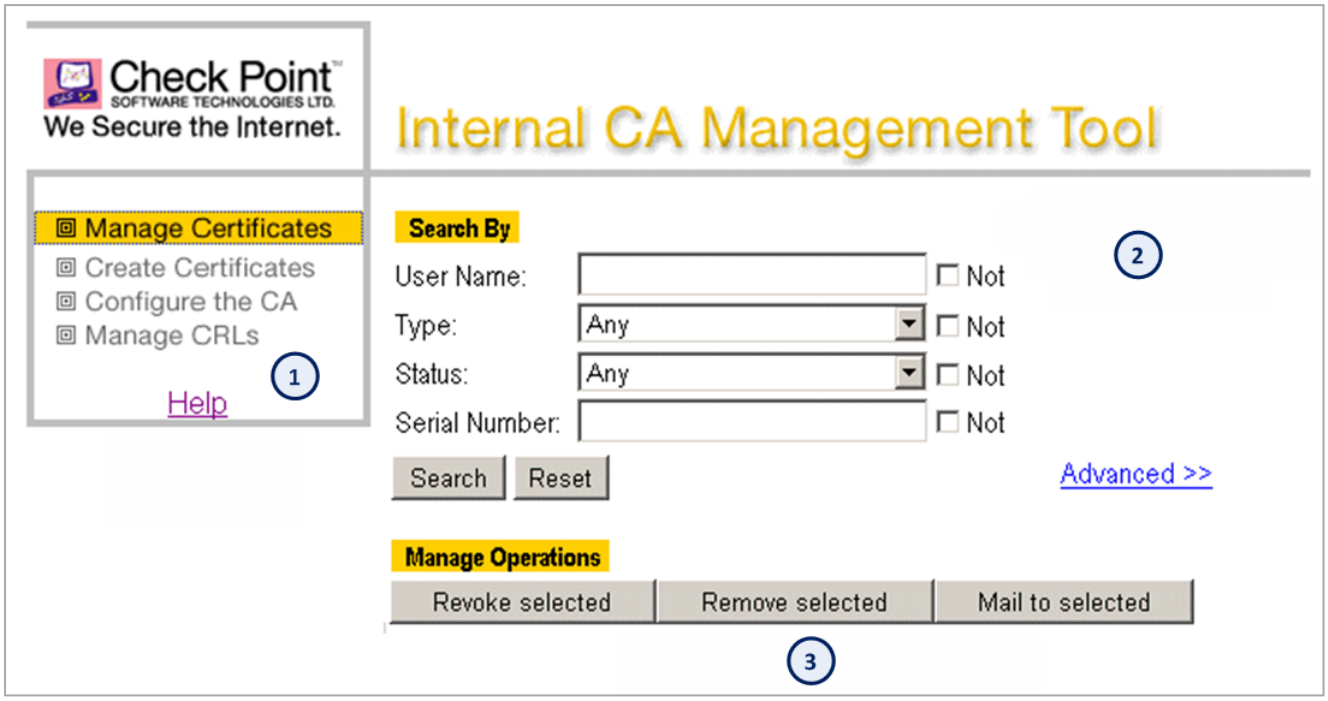
Identification
```

```
The Web site you want to view requests identification.

Select the certificate to use when connecting.
```

8. ICA管理ツールの認証に適した証明書を選択します。
9. **OK**をクリックします。
10. **Security Alert**ダイアログボックスで、**Yes**をクリックします。

ICA管理ツールポータル



項目	ペイン	説明
1	ホーム	操作一覧を表示します。
2	オペレーション	■ **証明書の管理** このペインでは、既存の証明書を管理します。 ウィンドウは、**Search attributes configuration**と**Bulk operation configuration**に分かれています。 ■ **証明書の作成** このペインでは、新しい証明書を作成できます。 ■ **CAの設定** このペインでは、内部認証局のパラメータを設定できます。 また、CAの時刻、名前、Security Management Serverのバージョンとビルド番号も表示できます。 ■ **CRLの管理** このペインでは、CRLのダウンロード、公開、再作成を行うことができます。
3	結果	適用された操作の結果を表示します。 このウィンドウは、証明書と証明書の属性のリストを含む表で構成されています。

ユーザ証明書の管理

内部で管理されているユーザ証明書は、ICA管理ツールを用いて初期化、失効、登録削除を行うことができます。LDAPサーバで管理されているユーザのユーザ証明書は、ICA管理ツールでのみ管理することができます。

この表は、ICA管理ツールで設定可能なユーザ証明書の属性を示しています。

属性	デフォルト	設定可能	コメント
有効	2年	yes	
キーサイズ	2048ビット	yes	4096ビットまで設定可能
内部データベースで管理しているユーザ証明書のDN	CN=ユーザ名、OU=ユーザ	no	このDNはICAのDNに付加される
LDAPサーバで管理されているユーザ証明書のDN		yes	LDAPブランチに依存
KeyUsage	5	yes	デジタル署名とキーの暗号化
ExtendedKeyUsage	0 (KeyUsageなし)	yes	

ユーザ証明書のキーサイズの変更

ユーザがリモートアクセスのマシンから登録を完了した場合、SmartConsoleの**詳細設定**ページでキーサイズを設定できます。

キーサイズを設定するには

1. **Menu**から、**Global Properties**を選択します。
2. 詳細設定に移動し、**Advanced Configuration**セクションで、**configure**をクリックします。

   Advanced Configurationウィンドウが開きます。
3. **Certificates and PKI properties**ページに移動します。
4. このプロパティの新しいキーサイズを設定します(`user_certs_key_size`)。
5. クリック**OK**。

キーサイズの変更も可能：*Database Tool (GuiDBEdit Tool)*。`users_certs_key_size Global Property`に記載されているように、キーサイズを変更します。サイトの更新時に新しい値がダウンロードされます。

複数の同時操作の実行

ICA管理ツールは、同時に複数の操作を行うことができます。例：

- LDAPクエリを実行し、全組織の従業員の詳細を確認する
- このデータからファイルを作成し、このファイルを使って
    - 全従業員の証明書作成を開始(初期化)する
    - 新しい証明書に関する通知を、従業員それぞれに送信する

次の操作は同時に行うことができます。

- ユーザ証明書の開始 (初期化)
- ユーザ証明書の失効
- ユーザへのメール送信
- 期限切れの証明書の削除
- 登録手続きが完了していない証明書の削除

権限が制限されたICA管理者

ICA管理ツールでは、制限された権限を持つ管理者をサポートしています。これらの管理者は複数の操作を同時に実行することはできず、権限には以下が含まれます。

- 基本的な検索
- 新規ユーザの証明書の初期化

証明書による運用

SIC証明書の管理

SICの証明書は、SmartConsoleで管理します。

セキュリティゲートウェイVPN証明書の管理

VPN証明書は、対応するネットワークオブジェクトのVPNページで管理されます。これらの証明書は、Check Point Security Gatewayまたはホストに対してIPsec VPN Bladeを定義すると、自動的に発行されます。この定義は、対応するネットワークオブジェクトの**一般プロパティ**ウィンドウで指定します。

VPN証明書が失効した場合、新しい証明書が自動的に発行されます。

SmartConsoleでのユーザ証明書の管理

内部データベースで管理しているユーザのユーザ証明書は、SmartConsoleで管理します。

詳細は、*ユーザ証明書*を参照：*R82 Remote Access VPN Administration Guide*。

証明書の初期化に関するユーザへの通知

ICA管理ツールでは、証明書の初期化に関する通知をユーザに送信するように設定できます。

メール通知を送信するには

1. メニューペインで、**Configure the CA**をクリックします。
2. **Management Tool Mail Attributes**領域で、次を設定します。
   - メールサーバ
   - メール"`From`"アドレス
   - オプションの"`To`"アドレス。ユーザのアドレスが不明な場合に使用することができます。

     管理者は、このアドレスを使って、ユーザに代わって証明書を取得し、後で転送することができます。
3. クリック**Apply**。

ICA証明書ファイルの取得

参照：*cpca_client set_ca_services (732ページ)*。

証明書の検索

検索方法は2つあります。

- ユーザ名、タイプ、ステータス、シリアル番号のみを含む基本的な検索方法
- すべての検索フィールドを含む詳細検索(無制限の権限を持つ管理者のみが実行可能)

証明書検索を行うには

Manage Certificatesページで、検索パラメータを入力し、Searchをクリックします。

基本検索パラメータ

- User Name- ユーザ名の文字列 (デフォルトではこのフィールドは空)
- Type-ドロップダウンリストには以下のオプションがあります:
  - *任意*(デフォルト)
  - *SIC*
  - *ゲートウェイ*
  - *内部ユーザまたはLDAPユーザ*
- Status-ドロップダウンリストには以下のオプションがあります:
  - *任意*(デフォルト)
  - *保留中*
  - *有効*
  - *取り消された*
  - *期限切れ*
  - *リニューアル*
- Serial Number- 要求された証明書のシリアル番号(デフォルトでは、このフィールドは空)

詳細検索の属性

基本検索のパラメータに加え、以下のパラメータを指定します。

- Sub DN- DN部分文字列(デフォルトでは、このフィールドは空)
- Valid From- 証明書が有効な日付。dd-mmm-yyyy [hh:mm:ss]の形式(例:15-Jan-2003) (デフォルトでは、このフィールドは空)
- Valid To- 証明書の有効期限をdd-mmm-yyyy [hh:mm:ss]の形式で指定(例:14-Jan-2003 15:39:26) (デフォルトではこのフィールドは空)
- CRL Distribution Point-ドロップダウンリストには以下のオプションがあります:

- *任意*(デフォルト)
- *CRL配布ポイントがない*(管理アップグレード前に発行された証明書、つまり旧CRLモードの証明書)

リストには利用可能なすべてのCRL番号も表示されます。

検索結果

検索結果はSearch Resultsペインに表示されます。このペインは、検索した証明書の属性の一覧表で構成されています。

- (SN) Serial Number- 証明書のSN
- User Name (CN)- 最初の等号("=")と次のコンマ(",")の間の文字列
- DN
- Status- 次のいずれか: *申請中*、*有効*、*失効*、*失効*、*更新(期限切れ)*
- 証明書が有効な日から、その証明書が失効する日までの日付

注 - ステータスバーには、各検索の後に検索統計が表示されます。

証明書の詳細の表示と保存

検索結果に表示される証明書の詳細を表示したり、保存したりすることができます。

証明書の詳細を表示および保存するには

検索結果ペインでDNリンクをクリックします。

- ステータスが*保留中*の場合、証明書情報と登録キーが表示され、ログエントリが作成され、SmartConsole >**Logs & Events** >**Logs** に表示されます。
- すでに証明書が作成されている場合は、ディスクに保存するか、直接開くことができます(オペレーティングシステムがファイル拡張子を認識している場合)。

証明書の削除と失効、およびEメールによる通知

1. メニューペインで、**Manage Certificates**をクリックします。
2. 設定された属性を持つ証明書を検索します (*証明書の検索 (648ページ)*)。

   結果が**Search Results**ペインに表示されます。
3. 必要に応じて証明書を選択し、これらのオプションのいずれかをクリックします。
   - **Revoke Selected**- 選択した証明書を失効させ、保留中の証明書をCAのデータベースから削除します。

- **Remove Selected**- 選択された証明書をCAのデータベースとCRから削除します。

  注 - 期限切れまたは保留中の証明書のみ削除することができます。

- **Mail to Selected**- 選択したすべての*保留中*の証明書に対してメールを送信

  メールには認証コードが記載されています。Eメールが定義されていないユーザへのメッセージは、デフォルトのアドレスに送信されます。詳細：*証明書の初期化に関するユーザへの通知 (648ページ)*。

CAへの証明書要求の送信

CAへの証明書リクエストの送信方法は3通りあります。

- **開始** - 登録キーがCA上で作成され、ユーザが証明書を作成する際に一度だけ使用します。
- **生成** - 証明書ファイルが作成され、証明書へのアクセス時に入力が必要なパスワードと関連付けられます。
- **PKCS#10** - CA がPKCS#10 の要求を受け取ると、証明書が作成され、要求者に引き渡されます。

証明書を発行するには

1. メニューペインで、**Create Certificates > Initiate**を選択します。
2. **User Name**または**Full DN**を入力するか、**Advanced**をクリックして、フォームに必要事項を入力します。
   - **Certificate Expiration Date**- 日付を選択するか、dd-mmm-yyyy[hh:mm:ss]のフォーマットで日付を入力します(デフォルト値は作成日から2年) 。
   - **Registration Key Expiration Date**- 日付を選択するか、dd-mmm-yyyy [hh:mm:ss]のフォーマットで日付を入力します(デフォルト値は作成日から2週間) 。
3. **Go**をクリックします。

   登録キーが作成され、**Results**ペインに表示されます。

   必要に応じて、**Send mail to user**をクリックして、登録キーをEメールで送信します。メールの文字数は1900字までです。
4. 正しい登録キーを入力すると、証明書が使用できるようになります。

証明書を生成するには

1. メニューペインで、**Create Certificates > Generate**を選択します。
2. **User Name**または**Full DN**を入力するか、**Advanced**をクリックして、フォームに必要事項を入力します。

- **Certificate Expiration Date**- 日付を選択するか、`dd-mm-yyyy [hh:mm:ss]` (デフォルト値は作成日から2年) のフォーマットで日付を入力します。
- **Registration Key Expiration Date**- 日付を選択するか、`dd-mm-yyyy [hh:mm:ss]` (デフォルト値は作成日から2週間) のフォーマットで日付を入力します。

3. パスワードを入力します。
4. **Go**をクリックします。
5. P12ファイルを保存し、ユーザに提供します。

PKCS#10 証明書を作成するには

1. メニューペインで、**Create Certificates > PKCS#10**を選択します。
2. 提供された暗号化されたBase-64バッファのテキストをスペースに貼り付けます。

   また、**Browse for a file to insert (IE only)**をクリックすると、リクエストファイルをインポートすることができます。
3. **Create**をクリックし、作成した証明書を保存します。
4. 証明書をリクエスト元に渡します。

複数の証明書の同時初期化

証明書を一括して初期化することができます。

複数の証明書を同時に初期化するには

1. 初期化するDNのリストをファイルとして作成します。

   注 - このファイルを作成するには、LDAPクエリによる方法とLDAP以外のクエリによる方法の2種類があります。
2. メニューのペインで、**Create Certificates > Advanced**にアクセスします。
3. 作成したファイルを参照します。
   - 登録キーをユーザに送信するには**Send registration keys via email**
   - 初期化されたDNとその登録キーをリストしたファイルを受け取るには、次を選択：**Save results to file**

     このファイルは、後でスクリプトで使用できます。
4. **Initiate from file**をクリックします。

LDAPクエリで作成されたファイル

LDAP検索で開始されたファイルは、このような形式になっています。

- 空白行またはファイルの先頭行以降の各行は、初期化されるDNを1つ表す
- 行頭が"mail="の場合、文字列は使用中のメールに続く

  Eメールが指定されていない場合、ICAの"Management Tool Mail To Address"属性からメールアドレスが取得されます。
- not_after属性の行がある場合、次の行の値は証明書の有効期限になる。

  日付は現在からの秒数で表示されます。
- otp_validity属性の行がある場合、次の行の値は登録キー有効期限になる。

  日付は現在からの秒数で表示されます。

以下は、LDAP検索の出力例です。

```
not_after
86400
otp_validity
3600
uid=user_1,ou=People,o=intranet,dc=company,dc=com
mail=user_1@company.com
<blank_line>
...
uid=...
```

詳細: *外部LDAPサーバ上のユーザの設定 (218ページ)*。

シンプルな非LDAPクエリで作成されたファイル

このフォーマットを使って、DN + メールをファイルに設定することで、簡単な(非LDAP) クエリを作成することが可能です。

```
<email address 1> space <DN 1>
... blank line as a separator ...
<email address 2> space <DN 2>
```

CRL

CRLの管理

デフォルトでは、CRLの有効期限は1週間です。この値は設定可能です。CRLは次のタイミングで発行されます。

- CRL有効期間の約60%が経過した場合
- 証明書の失効直後

ICA管理ツールで指定したCRLを再作成することができます。このユーティリティは、CRLが削除されたり破損したりした場合に、リカバリメカニズムとして機能します。管理者は、ICA管理ツールを使用して、DERエンコードされたバージョンのCRLをダウンロードすることができます。

CRLモード

ICAでは、複数のCRLを発行できます。複数のCRLを使用することで、1つのCRLが10Kより大きくなることを防ぎます。CRLが10Kを超えると、VPNトンネルを開こうとしたときにIKEネゴシエーションに失敗することがあります。

発行された各証明書を指定されたCRLに帰属させることで、複数のCRLが作成されます。失効した場合は、証明書のシリアル番号は指定されたCRLに表示されます。

証明書のCRL Distribution Point (CRLDP) 拡張子には、指定されたCRLのURLが含まれます。これにより、証明書が検証される際に正しいCRLが取得されます。

CRLの操作

CRLのダウンロード、更新、再作成は、ICA管理ツールから行えます。

CRLを使った操作を行うには

1. メニューペインで、**Manage CRLs**を選択します。
2. ドロップダウンボックスから、1つまたは複数のCRLを選択します。
3. アクションを選択します。
   - **Download**をクリックしてCRLをダウンロードします。
   - SmartConsoleセッションを公開するCRLデータベースに変更が加えられた後、CRLを更新します。

     この操作は、**CRL Duration**属性で設定された間隔で行われます。
   - **Recreate**をクリックして、CRLを再作成します。

CAプロシージャ

CAクリーンアップ

CAをクリーンアップするには、期限切れの証明書を削除する必要があります。期限切れの証明書は、手動または自動で削除できます。

期限切れの証明書を手動で削除するには

1. Security Management Serverで設定した時刻が正しいことを確認します。
2. メニューペインで、**Manage CRLs > Clean the CA's Database and CRLs from expired certificates**を選択します。

期限切れの証明書の自動削除

- 再起動するたびに、期限切れの証明書はすべて自動的に消去されます。
- また、自動クリーニング操作が3週間ごとに次の時間から開始するよう設定されています:
  - 初めてデバイスの電源を入れたとき。
  - デバイスで再起動を行うごとに。

CAの設定

CAを設定するには

1. メニューペインで、**Configure the CA**を選択します。
2. 次の*CAデータタイプと属性 (655ページ)*を必要に応じて編集します。
3. **Operations**ペインで、操作を選択します。
   - **Apply**- CAコンフィギュレーション設定を保存し、入力します。

     値が有効であれば、設定した内容はすぐに有効になります。無効な文字列はすべてデフォルト値に変更されます。
   - **Cancel**- すべての値を最後に保存した設定の値にリセットします。
   - **Restore Default**- CAをデフォルトの設定に戻します。

     属性の1つに文字列`Default`を入力して**Configure**をクリックすると、デフォルトにリセットされます。有効な値は要求に応じて変更され、その他の値はデフォルト値に変更されます。

CAデータタイプと属性

CAのデータタイプは次のとおりです。

- **Time** - `<number> days <number> seconds`, のような形式で表示されます: `CRL Duration: 7 days 0 seconds`

  数値は、表示される形式 (`<number> days <number> seconds`) または秒数で入力することができます。

- **Integer** - 通常の整数: `SIC Key Size: 2048`
- **Boolean** - 値はtrueまたはfalse(大文字と小文字は区別しない) : `Enable renewal: true`
- **String** - 英数字の文字列: `Management Tool DN prefix: cn=tests`

CAの属性をアルファベット順に並べると、このようになります。

属性	コメント	値	デフォルト
認証コードの長さ	認証コードの文字数。	最小-6 最大-12	6
CRLの有効期間	CRLが有効な期間。	最短-5分 最長-1年	1週間
リニューアルの有効化	ユーザ証明書の場合。更新の可否を示すブール値設定。	trueまたはfalse	true
失効までの猶予期間	古い証明書が更新された(置き換えられた)状態の時間。	*最小-0* *最長-5年*	1週間
猶予期間チェック期間	有効期間が過ぎたものを失効させるために、*Renewed(supersed)*リストを順次チェックする間の時間。	最短-10分 最長-1週間	1日
IKE証明書の有効期間	IKE証明書の有効期限。	最短-10分 最長-3年	1年
IKE証明書拡張キーの使用法	IKE証明書の拡張キー使用の種類を説明する証明書の目的。RFC 2459を参照してください。		KeyUsage がないことを意味します

属性	コメント	値	デフォルト
IKE証明書キーの使用	証明書の操作を説明する証明書の目的。RFC 2459を参照してください。		デジタル署名とキーの暗号化
管理ツールDNプレフィックス	ユーザ名を入力する際に作成されるDNのプレフィックスを決定します。	可能な値 CN= UID=	CN=
管理ツールのDN接尾辞	ユーザ名を入力する際に作成されるDNのサフィックスを決定します。		ou=users
管理ツールメールボタン非表示	セキュリティ上の理由から、証明書を1つ表示した後のメール送信ボタンを非表示にできます。	trueまたはfalse	false
管理ツールメールサーバ	登録コードメールを送信するために使用されるSMTPサーバ。デフォルトはなく、メール送信オプションを動作させるためには設定する必要があります。		-
管理ツール登録キー有効期間	管理ツールを使用して開始した場合の登録コードの有効期間。	最短-10分 最長-2ヶ月	2週間
管理ツールユーザ証明書の有効期間	管理ツールで開始した場合のユーザ証明書の有効期間。	最短-1週間 最長-20年	2年
管理ツールメール送信元アドレス	メール送信の際、**差出人**フィールドに表示されるメールアドレス。メール配信状況のレポートはこのアドレスに送信されます。		-
管理ツールメール件名	メールの件名フィールド。		-

属性	コメント	値	デフォルト
管理ツールメールテキスト形式	メッセージ本文に表示されるテキスト。`$REG_KEY`(ユーザ登録キー);`$EXPIRE`(有効期限)、`$USER`(ユーザのDN)。		登録キー: `$REG_KEY` Expiration: `$EXPIRE`
管理ツールメール宛先	メール**送信**オプションを使用すると、Eメールアドレスが定義されていないユーザへのメールは、このアドレスに送信されます。		-
配信ポイントあたりの最大証明書	新しいCRLモードでのCRLの最大容量。	最小-3 最大-400	400
新しいCRLモード	CRLモードを記述するブール値。	古いCRLモードの場合は0 新しいモードの場合は1	true
検索ページごとの証明書の数	検索ウィンドウの各ページに表示される証明書の数。	最小-1 最大-約700	約700
シリアル番号の桁数	証明書のシリアル番号の桁数。	最小-5 最大-10	5
更新された証明書の失効	このフラグは、更新された古い証明書を取り消すかどうかを決定します。これを取り消さない理由は、証明書が更新されるたびにCRLが増大するのを防ぐためです。 証明書が失効していない場合、ユーザは有効な証明書を2つ持つ可能性があります。	trueまたはfalse	true
SICキーサイズ	SICで使用するキーのビットサイズ。	可能な値: 1024 2048 4096	2048

属性	コメント	値	デフォルト
SIC証明書キーの使用	証明書の操作を説明する証明書の目的。RFC 2459を参照してください。		デジタル署名とキーの暗号化
SIC証明書の有効期間	SICの証明書の有効期間。	最短-10分 最長-20年	5年
ユーザ証明書拡張キーの使用法	ユーザ証明書の拡張キーの使用タイプを説明する証明書の目的。RFC 2459を参照してください。		KeyUsage がないことを意味します
ユーザ証明書の鍵のサイズ	ユーザの証明書のキーサイズ(ビット数)。	可能な値は次のとおりです。 1024 2048 4096	2048
ユーザ証明書の鍵の使用	証明書の操作を説明する証明書の目的。RFC 2459を参照してください。		デジタル署名とキーの暗号化

証明書の有効期限とステータス

ICAが発行する証明書には、有効期限が設定されています。期間が終了すると、証明書は*失効します*。

SIC証明書、セキュリティゲートウェイ用VPN証明書、ユーザ証明書をSmartConsoleでワンステップで作成することができます。ユーザ証明書は、SmartConsoleまたはICA管理ツールを使用して、2ステップで作成することもできます。2つのステップは次のとおりです。

- 初期化 - このステップで、ユーザの登録コードが作成されます。これが実行されると、証明書のステータスは*保留状態*になります。
- 登録 - ユーザがリモートクライアントで登録手続きを完了したとき。登録コードを入力すると、証明書が*有効*になります。

利点:

セキュリティ強化

- 秘密キーが作成され、ユーザのマシンに保存されます
- ICAが発行した証明書は、クライアントに安全にダウンロードされます。

発行前の証明書の自動削除および管理者による削除

ユーザが一定期間(デフォルトでは2週間)内に登録手続きを完了しない場合、登録コードは自動的に削除されます。管理者は、ユーザが登録手続きを完了する前に、登録キーを削除できます。その後、管理者はユーザ証明書を取り消すことができます。

ユーザ証明書の明示的または自動更新により、継続的なユーザ接続を確保

PKCS12型のユーザ証明書は、ユーザが明示的に更新できます。PKCS12証明書は、期限が切れると自動的に更新されるように設定することも可能です。この更新作業により、ユーザは継続的に組織のネットワークに接続できるようになります。古いユーザ証明書の自動失効を設定するタイミングは、管理者が選択できます。

もう1つの利点:

継続的なSIC接続を保証するSIC証明書の自動更新

SIC証明書は、証明書の有効期間の75%が経過すると自動的に更新されます。例えば、SICの証明書の有効期限が5年であった場合、3.75年経過後、新しい証明書が作成され、SICエンティティーに自動的にダウンロードされます。この自動更新により、セキュリティゲートウェイのSIC接続が継続的に確保されます。管理者は、古い証明書を自動的または一定期間後に取り消すことができます。デフォルトでは、古い証明書は証明書更新の1週間後に失効します。

Gaia API プロキシ

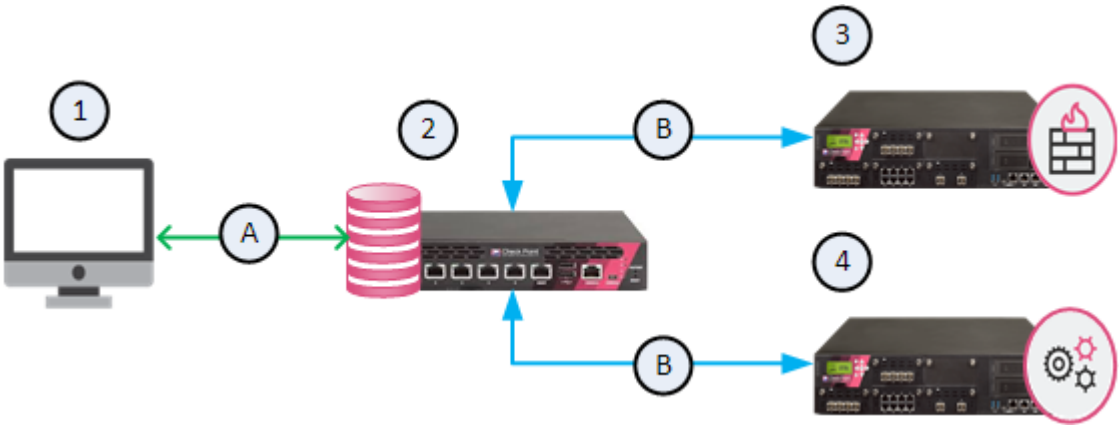
Check Point製品はAPIコマンドをサポートしています。詳細は*Check Point API Reference*。

管理サーバのGaia API プロキシ機能を使用すると、管理対象セキュリティゲートウェイとクラスタメンバで Gaia API コマンドを実行します。

1. 管理者は、APIクライアントを使用して管理サーバに接続します。
2. 管理サーバから、管理者は管理対象セキュリティーゲートウェイとクラスタメンバに対してGaia APIコマンドを実行します。

R82 Management Serverの Gaia API プロキシ機能は、Gaia API をサポートするすべてのマネージドセキュリティゲートウェイとクラスタメンバと連携します。

ダイアグラムの例



項目	説明
1	API クライアント
2	Gaia APIプロキシ機能を持つ管理サーバ
3	マネージドセキュリティゲートウェイ
4	管理対象ClusterXL
A	管理 API 通信
B	Gaia API コミュニケーション

重要 -スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) はこの機能をサポートしていません。(既知の制限 MBS-10832) 。

ワークフロー:

1. **管理API "login" コマンドを実行して、管理サーバにログインします。**

   APIクライアントを使用する場合は、Check Point APIの「login」コマンドを実行して管理サーバにログインします(「Check Point API の使用方法」を参照) 。*Check Point Management API Reference*)。

   重要 - ログインする管理者は、割り当てられた権限プロファイルで**Run One Time Script**権限が有効になっている必要があります。参照: *管理者への権限プロファイルの割り当て (116ページ)*。

2. **管理下のセキュリティゲートウェイとクラスタメンバでGaia APIコマンドを実行**

   管理 API "login" コマンドは、セッション一意識別子 (SID) トークンを返します。

   同じ API クライアントで、管理対象セキュリティゲートウェイとクラスタメンバで実行する Gaia API コマンドの "X-chkp-sid" フィールドでこの SID トークンを使用します。

   Gaia API 構文:

   ```
   POST https://<IP Address of Management Server>/web_api/gaia-api/<Gaia API Version>/<Gaia API Command>
   ```

   詳細は*Check Point Gaia API Reference*。

   Gaia API コマンドの本文は、以下のパラメータのいずれかによって、管理対象セキュリティゲートウェイまたはクラスタメンバを識別する必要があります。

   - オブジェクト名
   - オブジェクトプライマリ IP アドレス
   - オブジェクト UID

3. **Gaia API プロキシは指定されたセキュリティゲートウェイまたはクラスタメンバにログイン**

   管理サーバ上の Gaia API プロキシは Gaia API コマンドを解釈し、指定されたセキュリティゲートウェイまたはクラスタメンバにログインします。

   a. このログインは、セキュリティゲートウェイまたはクラスタメンバのSIDを返します。

   b. Gaia API プロキシはこの SID を使用して Gaia API コマンドを実行します。

c. Gaia API プロキシは、この SID をデータベースに保存します。

- 管理サーバの SID タイムアウトは 580 秒です。
- セキュリティゲートウェイまたはクラスタメンバの SID タイムアウトは 10 分です。

4. **Gaia APIプロキシは、セキュリティゲートウェイまたはクラスタメンバからの応答をAPIクライアントに転送します。**

- パフォーマンスを向上させるために、Gaia API プロキシはレスポンスを管理サーバの Gaia API プロキシキャッシュに保存します。
- Gaia API プロキシがキャッシュタイムアウト中に同じ Gaia API リクエストを受け取った場合、キャッシュから Gaia API レスポンスを返し、キャッシュを更新します。
- 管理者は、管理サーバ上の`$FWDIR/api/conf/cache.conf`ファイルで次のキャッシュパラメータを構成できます。

注 - `$FWDIR/api/conf/cache.conf`ファイルを変更したら、エキスパートモードで "`api reconf`" コマンドを使用して API サーバ設定を再読み込みする必要があります。

パラメータ	可能な値	説明
`timeout`	0またはそれ以上	次の Gaia API コマンドがその Gaia API コマンドのキャッシュ更新をトリガするまでの時間を指定します。 • `0`- Gaia APIプロキシはキャッシュを使用しません。 • *<integer>*- Gaia API プロキシは、Gaia API レスポンスを指定された秒数(デフォルト:60 秒)キャッシュに保存します。
`total_gateways`	整数	Gaia API レスポンスを保存する一意のセキュリティゲートウェイとクラスタメンバの数を指定します。
`maximum_entries`	整数	セキュリティゲートウェイとクラスタメンバごとに保存する一意のGaia API コマンドの数を指定します。

重要 - Gaia API プロキシは Gaia API コマンドを HTTPS 経由で送信します。セキュリティゲートウェイまたはClusterXLのアクセスコントロールポリシーは、管理サーバからセキュリティゲートウェイまたはクラスタメンバへの HTTPS トラフィックを明示的に許可する必要があります。

例

Gaia APIコマンド "show-hostname"

この例では、管理対象のセキュリティゲートウェイをオブジェクトのプライマリIPアドレスで識別します。

リクエスト

```
POST https://<IP Address of Management Server>/gaia-api/show-
hostname
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "192.168.1.1"
}
```

レスポンス

```
{
  "command-name" : "show-hostname",
  "response-message" : {
    "name" : "gw-832546"
  }
}
```

Gaia APIコマンド "show-interface"

この例では、管理対象 Security Gateway をオブジェクト名で識別します。

リクエスト

```
POST https://<IP Address of Management Server>/gaia-
api/v1.4/show-interfaces
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "gw-832546",
  "name" : "eth0"
}
```

レスポンス

```
{
  "command-name" : "v1.4/show-interfaces",
  "response-message" : {
    "ipv6-local-link-address": "Not Configured",
    "type": "physical",
    "name": "eth0",
    "ipv6-mask-length": "Not-Configured",
    "ipv6-address": "Not-Configured",
    "ipv6-autoconfig": "Not configured",
    "ipv4-address": "192.168.1.1",
    "enabled": true,
    "comments": "",
    "ipv4-mask-length": "24"
  }
}
```

Gaia APIコマンド "show-diagnostics"

この例では、管理対象のセキュリティゲートウェイをオブジェクト UID で識別します。

リクエスト

```
POST https://<IP Address of Management Server>/gaia-
api/v1.4/show-diagnostics
Content-Type: application/json
X-chkp-sid: <Session ID>
{
  "target" : "52048978-c507-8243-9d84-074d11154616",
  "category" : "os",
  "topic" : "disk"
}
```

レスポンス

```
{
  "command-name" : "v1.4/show-diagnostics",
  "response-message" : {
    "to": 3,
    "total": 3,
    "from": 1,
    "objects": [
      {
      "total": "34342961152",
      "partition": "/",
      "used": "5718065152",
      "free": "28624896000"
      },
      {
      "total": "304624640",
      "partition": "/boot",
      "used": "26991616",
      "free": "277633024"
      },
      {
      "total": "34342961152",
      "partition": "/var/log",
      "used": "455684096",
      "free": "33887277056"
      }
    ]
  }
}
```

SmartConsoleの新機能のテスト

ここに掲載されている新機能の中から1つ以上を選択してテストすることで、Check Pointの製品開発に影響を与えることができます。

SmartConsoleの新機能をテストするには

1. 左側のナビゲーションパネルでManage & Settingsをクリックします。。
2. Preferencesをクリックします。
3. Check Point Labセクション(一番下)で、テストしたい機能を選択します。
4. SmartConsoleセッションを公開する。

コマンドラインリファレンス

詳細は*R82 CLI Reference Guide*。

以下は、適用可能な限定的なコマンドのリストです。

CLIコマンドの構文凡例

可能な限り、このガイドには、コマンド、パラメータ、およびオプションがアルファベット順にリストされています。

このガイドでは、コマンドラインインタフェース(CLI) 構文でこの規則を使用します。

文字	説明

TAB	使用可能なネストされたサブコマンドを表示します。
	`main command`
	`→ nested subcommand 1`
	`→ → nested subsubcommand 1-1`
	`→ → nested subsubcommand 1-2`
	`→ nested subcommand 2`
	例:
	`cpwd_admin`
	`config`
	`-a <options>`
	`-d <options>`
	`-p`
	`-r`
	`del <options>`
	つまり、次のコマンドの**1つ**のみを実行できます。
	■ このコマンドを実行します。
	`cpwd_admin config -a <options>`
	■ または、次のコマンドを実行します。
	`cpwd_admin config -d <options>`
	■ または、次のコマンドを実行します。
	`cpwd_admin config -p`
	■ または、次のコマンドを実行します。
	`cpwd_admin config -r`
	■ または、次のコマンドを実行します。
	`cpwd_admin del <options>`

中括弧またはブレース **{}**	使用可能なコマンドまたはパラメータのリストを垂直バー**|** で区切って囲みます。 使用可能なコマンドまたはパラメータは1つのみ入力できます。

文字	説明
アングルブラケット **< >**	変数を囲みます。 ユーザは、サポートされる値を明示的に指定する必要があります。
大括弧またはブラケット **[ ]**	ユーザが入力できるオプションのコマンドまたはパラメータを囲みます。

contract_util

説明

Check Point Service Contractsと連動しています。

Service Contractファイルの詳細：sk33089: What is a Service Contract File?

構文

```
contract_util [-d]
    check <options>
    cpmacro <options>
    download <options>
    mgmt
    print <options>
    summary <options>
    update <options>
    verify
```

パラメータ

パラメータ	説明
check <options>	Security Gatewayがバージョンアップの対象かどうかを確認します。 参照：*contract_util check (673ページ)*。
cpmacro <options>	現在のcp.macroファイルを指定されたcp.macroファイルで上書きします。 参照：*contract_util cpmacro (674ページ)*。
download <options>	ユーザセンターまたはローカルファイルから、関連するすべてのCheck Point Service Contractsをダウンロードします。 参照：*contract_util download (675ページ)*。
mgmt	Management ServerからManaged Security GatewayにService Contractの情報を送ります。 参照：*contract_util mgmt (677ページ)*。
print <options>	インストールされているすべてのライセンスと、これらのライセンスがサービスコントラクトに含まれているかどうか、アップグレードの権利があるかどうかが表示されます。 参照：*contract_util print (678ページ)*。

パラメータ	説明
`summary <options>`	インストール後のサマリを表示します。 参照: *contract_util summary (679ページ)*。
`update <options>`	ユーザセンターのアカウントからCheck Point Service Contractsを更新します。 参照: *contract_util update (680ページ)*。
`verify`	Security Gatewayがバージョンアップの対象かどうかを確認します。 また、このコマンドは戻り値を解釈し、意味のあるメッセージを表示します。 参照: *contract_util verify (681ページ)*。

contract_util check

説明

Security Gatewayがバージョンアップの対象かどうかを確認します。

Service Contractファイルの詳細：sk33089: What is a Service Contract File?

構文

```
contract_util check
    {-h | -help}
    hfa
    maj_upgrade
    min_upgrade
    upgrade
```

パラメータ

パラメータ	説明
{-h | -help}	該当する組み込みの使用状況を表示します。
hfa	Security Gatewayがより新しいHotfix Accumulatorへのアップグレードの対象であるかどうかを確認します。
maj_upgrade	Security Gatewayが上位のメジャーバージョンへのアップグレードの対象であるかどうかを確認します。
min_upgrade	Security Gatewayが上位のマイナーバージョンへのアップグレードの対象であるかどうかを確認します。
upgrade	Security Gatewayがバージョンアップの対象かどうかを確認します。

contract_util cpmacro

説明

指定されたファイルが現在のファイルより新しい場合、現在の`cp.macro`ファイルを指定された`cp.macro`ファイルで上書きします。

`cp.macro`ファイルについての詳細：sk96217: What is a cp.macro file?

構文

```
contract_util cpmacro /<path_to>/cp.macro
```

このコマンドは、次のいずれかのメッセージを表示します。

メッセージ	説明
`CntrctUtils_ Write_cp_macro returned -1`	`contract_util cpmacro`コマンドは失敗しました。 ■ 一時ファイルの作成に失敗しました。 ■ 一時ファイルへの書き込みに失敗しました。 ■ 現在のファイルの置き換えに失敗しました。
`CntrctUtils_ Write_cp_macro returned 0`	`contract_util cpmacro`コマンドは、指定されたファイルの方が新しいので、現在のファイルを指定されたファイルで上書きすることができました。
`CntrctUtils_ Write_cp_macro returned 1`	`contract_util cpmacro`コマンドは、指定されたファイルより新しいため、現在のファイルを上書きしませんでした。

contract_util download

説明

ユーザセンターまたはローカルファイルから、関連するすべてのCheck Point Service Contractsをダウンロードします。

Service Contractファイルの詳細：sk33089: What is a Service Contract File?

構文

```
contract_util download
      {-h | -help}
      local
            {-h | -help}
            [{hfa | maj_upgrade | min_upgrade | upgrade}] <Service
Contract File>
      uc
            {-h | -help}
            [-i] [{hfa | maj_upgrade | min_upgrade | upgrade}]
<Username> <Password> [<Proxy Server> [<Proxy Username>:<Proxy
Password>]]
```

パラメータ

パラメータ	説明
`{-h | -help}`	該当する組み込みの使用状況を表示します。
`-i`	インタラクティブモード - ユーザセンターの認証情報とプロキシサーバの設定をユーザに要求します。
`local`	サービスコントラクトをローカルファイルからダウンロードします。 これは"`cplic contract put`"コマンドと同等です。 *cplic contract (752ページ)*)。
`uc`	ユーザセンターからサービスコントラクトをダウンロードします。
`hfa`	Hotfix Accumulatorに関する情報をダウンロードします。
`maj_upgrade`	メジャーバージョンに関する情報をダウンロードします。
`min_upgrade`	マイナーバージョンに関する情報をダウンロードします。
`upgrade`	アップグレードの情報をダウンロードします。
<Username>	ユーザセンターアカウントのEメールアドレス。
<Password>	ユーザセンターのアカウントパスワード。
<Proxy Server> [*<Proxy Username>*:*<Proxy Password>*]	ユーザセンターへの接続がプロキシサーバを経由することを指定します。 ■ *<Proxy Server>*- プロキシサーバの解決可能なホスト名のIPアドレス ■ *<Proxy Username>*- プロキシサーバのユーザ名。 ■ *<Proxy Password>*- プロキシサーバのパスワード。 注 - プロキシサーバを明示的に指定しない場合、コマンドは管理データベースで設定されたプロキシサーバを使用します。
<Service Contract File>	サービスコントラクトのファイルへのパスとファイル名。 まず、ユーザセンターのアカウントからサービスコントラクトファイルをダウンロードする必要があります。

contract_util mgmt

説明

Management ServerからManaged Security GatewayにService Contractの情報を送ります。

Service Contractファイルの詳細：sk33089: What is a Service Contract File?

構文

```
contract_util mgmt
```

contract_util print

説明

インストールされているすべてのライセンスと、これらのライセンスがサービスコントラクトに含まれているかどうか、アップグレードの権利があるかどうかが表示されます。

このコマンドは、サービスコントラクトファイルで認識されていないライセンスを表示することができます。

Service Contractファイルの詳細：sk33089: What is a Service Contract File?

構文

```
contract_util [-d] print
      {-h | -help}
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

パラメータ

パラメータ	説明
{-h | -help}	該当する組み込みの使用状況を表示します。
-d	フォーマットされたテーブルのヘッダと詳細情報を表示します。
hfa	Hotfix Accumulatorの情報が表示されます。
maj_upgrade	メジャーバージョンに関する情報を表示します。
min_upgrade	マイナーバージョンに関する情報を表示します。
upgrade	アップグレードに関する情報を表示します。

contract_util summary

説明

インストール後の概要と、このCheck Pointコンピュータがアップグレードの対象であるかどうかを表示します。

構文

```
contract_util summary
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

パラメータ

パラメータ	説明
hfa	Hotfix Accumulatorの情報が表示されます。
maj_upgrade	メジャーバージョンに関する情報を表示します。
min_upgrade	マイナーバージョンに関する情報を表示します。
upgrade	アップグレードに関する情報を表示します。

contract_util update

説明

ユーザセンターアカウントからCheck Pointサービスコントラクトを更新します。

Service Contractファイルの詳細：sk33089: What is a Service Contract File?

構文

```
contract_util update
      [-proxy <Proxy Server>:<Proxy Port>]
      [-ca_path <Path to ca-bundle.crt File>]
```

パラメータ

パラメータ	説明
`update`	ユーザセンターアカウントからCheck Pointのサービスコントラクト(プリインストールライセンスに付属)を更新します。
`-proxy <Proxy Server>:<Proxy Port>`	ユーザセンターへの接続がプロキシサーバを経由することを指定します。 ■ *<Proxy Server>*- プロキシサーバの解決可能なホスト名のIPアドレス。 ■ *<Proxy Port>*- プロキシサーバの該当するポート。 注 - プロキシを明示的に指定しない場合、コマンドは管理データベースで構成されたプロキシを使用します。
`-ca_path <Path to ca-bundle.crt File>`	認証局バンドルファイル(`ca-bundle.crt`)へのパスを指定します。 **注** - 明示的にパスを指定しない場合、コマンドはデフォルトのパスを使用します。

contract_util verify

説明

Security Gatewayがバージョンアップの対象かどうかを確認します。

このコマンドは*contract_util check (673ページ)*コマンドと同じですが、返り値を解釈し、意味のあるメッセージを表示します。

Service Contractファイルの詳細：sk33089: What is a Service Contract File?

構文

```
contract_util verify
```

cp_conf

説明

Check Point製品のインストールを構成または再設定します。

注 - 各Check Pointコンピュータで利用可能なオプションは、構成とインストールされている製品によって異なります。

管理サーバ上の構文

```
cp_conf
       -h
       admin <options>
       auto <options>
       ca <options>
       client <options>
       finger <options>
       lic <options>
       snmp <options>
```

パラメータ

パラメータ	説明
`-h`	ビルトインの使用状況全体を表示します。
`admin <options>`	Security Management Serverに対してCheck Pointのシステム管理者を設定します。 参照: *cp_conf admin (684ページ)*。
`auto <options>`	起動時のCheck Point製品の自動起動を表示および設定します。 参照: *cp_conf auto (687ページ)*。
`ca <options>`	■ 認証局(CA)の完全修飾ドメイン名(FQDN)を設定します。 ■ 内部認証局(ICA)を初期化します。 参照: *cp_conf ca (688ページ)*。
`client <options>`	SmartConsoleを使用してSecurity Management Serverに接続できるGUIクライアントを設定します。 参照: *cp_conf client (690ページ)*。

パラメータ	説明
`finger <options>`	ICAのフィンガープリントを表示します。 参照: *cp_conf finger (694ページ)*。
`lic <options>`	Check Pointライセンスを管理します。 参照: *cp_conf lic (695ページ)*。
`snmp <options>`	これらの古いコマンドは使用**しないで**ください。 SNMPを設定するには*R82 Gaia Administration Guide*- 章「*システム管理*」- セクション*SNMP*

cp_conf admin

説明

Security Management Serverに対してCheck Pointのシステム管理者を設定します。

注:

- Multi-Domain Serverはこのコマンドをサポートしていません。
- 1人の管理者だけが*cpconfig (743ページ)*メニュー) に該当します。
  管理者を追加定義するには、SmartConsoleを使用します。
- このコマンドは、オプション**Administrator**(*cpconfig (743ページ)*メニュー) に該当します。

構文

```
cp_conf admin
       -h
       add [<UserName> <Password> {a | w | r}]
       add -gaia [{a | w | r}]
       del <UserName1> <UserName2> ...
       get
```

パラメータ

パラメータ	説明
`-h`	該当する組み込みの使用状況を表示します。
`add [<UserName> <Password> {a | w | r}]`	Check Pointのシステム管理者を追加します。 ■ `<UserName>`- 管理者のユーザ名を指定します ■ `<Password>`- 管理者のパスワードを指定します ■ `a`- 設定の読み取り、設定の書き込み、管理者の管理など、すべての権限を割り当てる ■ `w`- 設定の読み取りと書き込みのみに権限を割り当てる(管理者は管理不可) ■ `r`- 読み取り設定のみに権限を割り当てる
`add -gaia [{a | w | r}]`	Gaia管理者ユーザ`admin`を追加します。 ■ `a`- 設定の読み取り、設定の書き込み、管理者の管理など、すべての権限を割り当てる ■ `w`- 設定の読み取りと書き込みのみに権限を割り当てる(管理者は管理不可) ■ `r`- 読み取り設定のみに権限を割り当てる
`del <UserName1> <UserName2> ...`	指定したシステム管理者を削除します。
`get`	設定されているシステム管理者の一覧を表示します。
`get -gaia`	Gaia administratorユーザ`admin`に割り当てられた管理権限を表示します。

例 1 - Check Pointのシステム管理者を追加する場合

```
[Expert@MGMT:0]# cp_conf admin add
Administrator name: admin
Administrator admin already exists.
Do you want to change Administrator's Permissions (y/n) [n] ? y

Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w

Administrator admin was modified successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; )
[Expert@MGMT:0]#
```

例2 - Gaiaの管理者ユーザを追加する場合

```
[Expert@MGMT:0]# cp_conf admin add -gaia
Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w
Administrator admin was added successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get -gaia

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; ) - Gaia admin
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia a
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products with Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia w
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products without Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia r
Administrator admin already exists.

Administrator admin was modified successfully and has
Read Only Permission for all products
[Expert@MGMT:0]#
```

cp_conf auto

説明

起動時に自動的に起動するCheck Point製品を表示および制御します。

注 - このコマンドは、オプション**Automatic start of Check Point Products**(*cpconfig (743 ページ)*メニュー) に該当します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

パラメータ

パラメータ	説明
`-h`	該当する組み込みの使用状況を表示します。
`{enable | disable} <Product1> <Product2> ...`	インストールされているCheck Point製品を、起動時に自動的に起動するかどうかを制御します。 このコマンドはCheck Pointでのみ使用されます。
`get all`	Check Point製品のうち、起動時に自動的に起動するものを表示します。 ■ Check Point Security Gateway ■ QoS (旧FloodGate-1) ■ SmartEvent Suite

Security Management Serverからの例

```
[Expert@MGMT:0]# cp_conf auto get all
Check Point Security Gateway is not installed

QoS is not installed

The SmartEvent Suite will start automatically at boot time.

[Expert@MGMT:0]#
```

cp_conf ca

説明

このコマンドは、内部認証局(ICA)の設定を変更します。

注 - Security Management Serverでは、このコマンドはオプション**Certificate Authority**(*cpconfig (743ページ)*メニュー)に該当します。

構文

```
cp_conf ca
       -h
       fqdn <FQDN Name>
       init
```

パラメータ

パラメータ	説明
`-h`	該当する組み込みの使用状況を表示します。
`fqdn <FQDN Name>`	内部認証局(ICA)の完全修飾ドメイン名(FQDN)を設定します。"`<FQDN Name>`"は、*hostname.domainname*形式の文字列です。 **注:** ■ 構成されたオブジェクトの既存の証明書は失効**しません**。 ■ 既存のICA証明書は変更**されません**。 ■ 管理サーバは、指定された「`<FQDN Name>`」を使用して、ICAが生成するすべての証明書にCRL DP(Certificate Revocation List Distribution Point)プロパティを設定します。 このコマンドを参照: *cpca_client get_crldp (719ページ)*
`init`	内部認証局(ICA)を初期化します。

例

```
[Expert@MyMGMT:0]# hostname
MyMGMT
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# domainname
checkpoint.com
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# cp_conf ca fqdn MyMGMT.checkpoint.com
Trying to contact Certificate Authority. It might take a while...
Certificate was created successfully
MyMGMT.checkpoint.com was successfully set to the Internal CA
[Expert@MyMGMT:0]#
```

cp_conf client

説明

SmartConsoleでSecurity Management Serverへの接続を許可するGUIクライアントを設定します。

注:

- Multi-Domain Serverはこのコマンドをサポートしていません。
- このコマンドは、オプション**GUI Clients**(*cpconfig (743ページ)*メニュー) に該当します。

構文

```
cp_conf client
      add <GUI Client>
      createlist <GUI Client 1> <GUI Client 2> ...
      del <GUI Client 1> <GUI Client 2> ...
      get
```

パラメータ

パラメータ	説明
-h	ビルトインの使用状況を表示します。
<GUI Client>	*<GUI Client>*次のいずれか: ■ 1つのIPv4アドレス(例えば192.168.10.20) 、または1つのIPv6アドレス(例えば3731:54:65fe:2::a7) ■ 1つのホスト名 (例えばMyComputer) ■ "Any"- すべてのIPv4およびIPv6アドレスを無制限に表記するには ■ IPv4アドレスの範囲 (例えば192.168.10.0/255.255.0) 、またはIPv6アドレスの範囲 (例えば2001::1/128) ■ IPv4アドレスのワイルドカード (例えば192.168.10.*)
add *<GUI Client>*	GUIクライアントを追加します。
createlist *<GUI Client 1> <GUI Client 2> ...*	現在許可されているGUIクライアントを削除し、許可されているGUIクライアントのリストを新規に作成します。
del *<GUI Client 1> <GUI Client 2> ...*	指定されたGUIクライアントを削除します。
get	許可されたGUIクライアントを表示します。

例

例1 - 1つのIPv4アドレスを設定する

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.15
172.20.168.15 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.15
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.15
172.20.168.15 was deleted successfully
[Expert@MGMT:0]#
```

例2 - 1つのホスト名を設定する

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add MySmartConsoleHost
MySmartConsoleHost was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
MySmartConsoleHost
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del MySmartConsoleHost
MySmartConsoleHost was deleted successfully
[Expert@MGMT:0]#
```

例3 - "Any"を設定する

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add "Any"
Any was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del "Any"
Any was deleted successfully
[Expert@MGMT:0]#
```

例4 - IPv4アドレスの範囲を設定する

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was deleted successfully
[Expert@MGMT:0]#
```

例5 - IPv4アドレスワイルドカードの設定

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.*
172.20.168.* was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.*
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.*
172.20.168.* was deleted successfully
[Expert@MGMT:0]#
```

例6 - 現在のリストを削除し、許可されたGUIクライアントの新しいリストを作成

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist 192.168.40.0/255.255.255.0 172.30.40.55
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
192.168.40.0/255.255.255.0
172.30.40.55
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist "Any"
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#
```

cp_conf finger

説明

内部認証局のフィンガープリントを表示します。

このフィンガープリントは、Security Management Server、Multi-Domain Server、Domain Management Server上のICA証明書からのテキスト文字列です。

このフィンガープリントは、SmartConsoleで接続する際に、Security Management Server、Multi-Domain Server、またはDomain Management Serverのアイデンティティを検証します。

注 - このコマンドは、オプション**Certificate's Fingerprint**(*cpconfig (743ページ)*メニュー) に該当します。

構文

```
cp_conf finger
      -h
      get
```

パラメータ

パラメータ	説明
-h	該当する組み込みの使用状況を表示します。
get	ICAのフィンガープリントを表示します。

例

```
[Expert@MGMT:0]# cp_conf finger get
EDNA COCO MOLE ATOM ASH MOT SAGE NINE ILL TINT HI CUBE
[Expert@MGMT:0]#
```

cp_conf lic

説明

Check Pointライセンスの表示、追加、削除を行います。

注 - このコマンドは、オプション**Licenses and contracts**(*cpconfig (743ページ)*メニュー) に該当します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

パラメータ

パラメータ	説明
`-h`	該当する組み込みの使用状況を表示します。
`add -f <Full Path to License File>`	指定されたCheck Pointライセンスファイルからライセンスを追加します。 このライセンスファイルは*Check Point User Center*。 これは*cplic db_add (754ページ)*。
`add -m <Host> <Date> <Signature Key> <SKU/Features>`	ライセンスを手動で追加します。 ライセンスの詳細は*Check Point User Center*。 これは*cplic db_add (754ページ)*。
`del <Signature Key>`	シグネチャに基づきライセンスを削除します。 これは*cplic del (759ページ)*。
`get [-x]`	ローカルにインストールされているライセンスが表示されます。 "`-x`"パラメータを指定した場合、インストールされているすべてのライセンスのシグネチャキーも出力されます。 これは*cplic print (763ページ)*。

例1 - ファイルからライセンスを追加する

```
[Expert@HostName:0]# cp_conf lic add -f ~/License.lic
License was installed successfully.
[Expert@HostName:0]#

[Expert@HostName:0]# cp_conf lic get
Host             Expiration   Signature                                   Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@HostName:0]#
```

例2 - ライセンスを手動で追加する

```
[Expert@MyHostName:0]# cp_conf lic add -m MyHostName 25Aug2019
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX
License was successfully installed
[Expert@MyHostName:0]#

[Expert@MyHostName:0]# cp_conf lic get
Host             Expiration   Signature                                   Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@MyHostName:0]#
```

cp_log_export

説明

Check Pointのログをsyslog経由でエクスポートします。

詳しくは次を参照してください: sk122323および*R82 Logging and Monitoring Administration Guide*。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cp_log_export
cp_log_export <command-name> help
```

パラメータ

パラメータ	説明
パラメータなし	組み込みの一般的なヘルプを表示します。
`<command-name> help`	特定の内部コマンドの組み込みヘルプを表示します。

内部コマンド

名前	説明
add	新しいCheck Point Log Exporterを設定します。 `cp_log_export add name <Name> target-server <Target-Server> target-port <Target-Server-Port> protocol {udp | tcp} [Optional Arguments]`
delete	既存のLog Exporterを削除します。 `cp_log_export delete name <Name>`

reexport	現在のログ位置をリセットし、設定に基づき再度すべてのログをエクスポートします。
	`cp_log_export reexport name <Name> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Last Exported Log> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Gap Start> end-position <Position of Gap End> --apply-now`

restart	Log Exporterプロセスを再起動します。 `cp_log_export restart name <Name>`
set	既存のLog Exporterの設定を更新します。 `cp_log_export set name <Name> [<Optional Arguments>]`
show	現在のLog Exporterの設定を表示します。 `cp_log_export show [<Optional Arguments>]`
start	既存のLog Exporterプロセスを開始します。 `cp_log_export start name <Name>`
status	Log Exporterの概要ステータスを表示します。 `cp_log_export status [<Optional Arguments>]`
stop	既存のLog Exporterのプロセスを停止します。 `cp_log_export stop name <Name>`

内部コマンドの引数

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`--apply-now`	`add", "set", "delete", "reexport"`コマンドで行われた変更をすぐに適用します。	任意	任意	**必須**	N/A	N/A	**必須**
`ca-cert <Path>`	CA証明書ファイル `*.pem`へのフルパスを指定します。 **重要** - 引数 `"encrypted"`の値が`"true"`の場合のみ適用されます。	任意	任意	N/A	N/A	N/A	N/A
`client-cert <Path>`	クライアント証明書 `*.p12`のフルパスを指定します。 **重要** - 引数 `"encrypted"`の値が`"true"`の場合のみ適用されます。	任意	任意	N/A	N/A	N/A	N/A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`client-secret <Phrase>`	クライアント証明書 `*.p12`の作成に使用するチャレンジフレーズを指定します。 **重要** - 引数 "`encrypted`"の値が"`true`"の場合のみ適用されます。	任意	任意	N/A	N/A	N/A	N/A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`domain-server {mds | all}`	マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストを指定します。 マルチドメインログサーバでは、該当するドメインログサーバコンテキストを指定します。 **重要:** ■ "mds" (小文字) - メイン **MDS**レベルのみからすべてのログをエクスポートします。 ■ "all" (小文字) - **すべて**のドメインからすべてのログをエクスポートします。	**必須**	**必須**	**必須**	N/A	任意	**必須**
`enabled {true | false}`	デフォルト:`true`	任意	任意	N/A	N/A	N/A	N/A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`encrypted {true | false}`	ログの送信にTSL (SSL) 暗号化を使用するかどうかを指定します。 デフォルト:`false`	任意	任意	N/A	N/A	N/A	N/A
`end-position <Position>`	ログをエクスポートする終了位置を指定します。	N/A	N/A	N/A	N/A	N/A	任意
`export-attachment-ids {true | false}`	エクスポートされたログに、ログの添付のIDを表すフィールドを追加するかどうかを指定します (存在する場合)。 デフォルト:`false`	任意	任意	N/A	N/A	N/A	N/A
`export-attachment-link {true | false}`	ログカードを表示し、自動的に添付ファイルを開くSmartViewへのリンクを表すフィールドを、エクスポートされたログに追加するかどうかを指定します。 デフォルト:`false`	任意	任意	N/A	N/A	N/A	N/A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`export-link {true | false}`	ログカードを表示するSmartViewへのリンクを表すフィールドを、エクスポートされたログに追加するかどうかを指定します。 デフォルト:`false`	任意	任意	N/A	N/A	N/A	N/A
`export-link-ip {true | false}`	SmartViewへのリンクにカスタムIPアドレスを使用させるかどうかを指定します(NAT背後のLog Serverの場合など)。 **重要** - 引数"`export-link`"の値が"`true`"、または引数"`export-attachment-link`"の値が"`true`"の場合のみ適用されます。 デフォルト:`false`	任意	任意	N/A	N/A	N/A	N/A
`export-log-position {true | false}`	ログの位置をエクスポートするかどうかを指定します。 デフォルト:`false`	任意	任意	N/A	N/A	N/A	N/A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`filter-action-in {"Action1","Action2",... | false}`	"Action"フィールドに特定の値を含むすべてのログをエクスポートするかどうかを指定します。 各値は二重引用符 ("") で囲む必要があります。 複数の値がサポートされ、スペースなしのカンマで区切る必要があります。 すべての有効な値を確認するには 1. SmartConsoleで、**Logs & Events**ビューで、**Logs**タブを開きます。 2. 一番上のクエリフィールドに、**action:**と一文字入力します。 値の例: ■ **Accept** ■ **Block** ■ **Bypass** ■ **Detect** ■ **Drop**	任意	任意	N/A	N/A	N/A	N/A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
	■ HTTPS Bypass ■ HTTPS Inspect ■ Prevent ■ Reject **重要** - このパラメータは、フィルタリングXMLファイル内でこのフィールドに対して先に直接宣言された他のフィルタリング設定を置き換えます。他のフィールドフィルタは上書きされません。						

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`filter-blade-in {"Blade1","Blade2",... | false}`	**Blade**"フィールドに特定の値を含むすべてのログをエクスポートするかどうかを指定します (これらのログを生成した Software Bladeのオブジェクト名)。 各値は二重引用符 ("") で囲む必要があります。 複数の値がサポートされ、スペースなしのカンマで区切る必要があります。 すべての有効な値を確認するには 1. SmartConsole で、**Logs & Events**ビューで、**Logs**タブを開きます。 2. 一番上のクエリフィールドに、**blade:**と一文字入力します。 値の例: ■ **Anti-Bot** ■ **Firewall**	任意	任意	N/A	N/A	N/A	N/A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
	■ HTTPS Inspection ■ Identity Awareness ■ IPS 有効なSoftware Blade ファミリ: ■ Access ■ TP ■ Endpoint ■ Mobile **重要** - このパラメータは、フィルタリングXMLファイル内でこのフィールドに対して先に直接宣言された他のフィルタリング設定を置き換えます。他のフィールドフィルタは上書きされません。						

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`filter-origin-in {"Origin1","Origin2",... | false}`	"Origin"フィールドに特定の値 (これらのログを生成したSecurity Gateway / クラスタメンバのオブジェクト名) を含むすべてのログをエクスポートするかどうかを指定します。 各原点値は二重引用符 ("") で囲む必要があります。 複数の値がサポートされ、スペースなしのカンマで区切る必要があります。 **重要** - このパラメータは、フィルタリングXMLファイル内でこのフィールドに対して先に直接宣言された他のフィルタリング設定を置き換えます。他のフィールドフィルタは上書きされません。	任意	任意	N / A	N / A	N / A	N / A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`format {generic | cef | json | leef | logrhythm | rsa | splunk | syslog}`	ログをエクスポートする形式を指定します。 デフォルト:`syslog`	任意	任意	N/A	N/A	N/A	N/A
`name "<Name>"`	Log Exporter設定の一意の名前を指定します。 **注:** ■ 使用できる文字:ラテン文字、数字 ("`0-9`")、マイナス ("`-`")、アンダースコア ("`_`")、ピリオド ("`.`") ■ 最初は文字で始めます。 ■ 最小文字数は2文字です。 ■ `add`"コマンドは、`$EXPORTERDIR/targets/`ディレクトリに、指定した一意名で新しいターゲットディレクトリを作成します。	**必須**	**必須**	**必須**	オプションです。デフォルトでは、すべてに適用されます。	オプションです。デフォルトでは、すべてに適用されます。	**必須**

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`protocol {tcp | udp}`	使用するレイヤー4トランスポートプロトコル (TCPまたはUDP) を指定します。 デフォルト値はありません。	**必須**	任意	N/A	N/A	N/A	N/A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`read-mode {raw | semi-unified}`	ログファイルを読み込むモードを指定します。 ■ `raw`- Log Exporterを使用してログ記録を単一化せずにエクスポートすることを指定します。 ■ `semi-unified`- Log Exporterを使用してログ記録を段階的に統一してエクスポートすることを指定します。つまり、各ログ記録に対して、過去に出会った同じIDを持つ記録を統一した記録をエクスポートします。 デフォルト:`semi-unified` デフォルト:`raw`	任意	任意	N/A	N/A	N/A	N/A

名前	説明	必要 "add" コマンド	必要 "set" コマンド	必要 "delete" コマンド	必要性 "reconf" コマンド	必要性 "restart", "show", "status", "start"、"stop" コマンド	必要 "reexport" コマンド
`reconnect-interval {<Number> | default}`	接続が失われた後、Log Exporterがターゲットサーバに再接続する間隔(分)。 無効にする場合は、"`default`"を入力します。 デフォルト値はありません。	任意	任意	N/A	N/A	N/A	N/A
`start-position <Position>`	ログをエクスポートする開始位置を指定します。	N/A	N/A	N/A	N/A	N/A	任意
`target-port <Target-Server-Port>`	ログのエクスポート先であるターゲットサーバのリスニングポートを指定します。	**必須**	任意	N/A	N/A	N/A	N/A
`target-server <Target-Server>`	ログのエクスポート先となるターゲットサーバのIPアドレスまたはFQDNを指定します。	**必須**	任意	N/A	N/A	N/A	N/A
`time-in-milli {true | false}`	時間分解能をミリ秒単位で指定してログをエクスポートするかどうかを指定します。 Security Gateway R81以降が必要です。 デフォルト:`false`	任意	任意	N/A	N/A	N/A	N/A

cpca_client

説明

内部認証局(ICA)に対する操作を実行します。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d]
      create_cert <options>
      double_sign <options>
      get_crldp <options>
      get_pubkey <options>
      init_certs <options>
      lscert <options>
      revoke_cert <options>
      revoke_non_exist_cert <options>
      search <options>
      set_ca_services <options>
      set_cert_validity <options>
      set_mgmt_tool <options>
      set_sign_hash <options>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`create_cert <options>`	Security Management ServerまたはDomain Management Server用のSIC証明書を発行します。 参照: *cpca_client create_cert (715ページ)*。

パラメータ	説明
`double_sign <options>`	証明書の2つ目の署名を作成します。 参照: *cpca_client double_sign (717ページ)*。
`get_crldp <options>`	CRL配布ポイントからCRLファイルにアクセスする方法を示します。 参照: *cpca_client get_crldp (719ページ)*。
`get_pubkey <options>`	ICAの証明書の公開鍵のエンコードをファイルに保存します。 参照: *cpca_client get_pubkey (720ページ)*。
`init_certs <options>`	ユーザのDNリストをインポートし、各ユーザの登録キーを含むファイルを作成します。 参照: *cpca_client init_certs (721ページ)*。
`lscert <options>`	ICAが発行したすべての証明書を表示します。 参照: *cpca_client lscert (722ページ)*。
`revoke_cert <options>`	ICAが発行した証明書を取り消します。 参照: *cpca_client revoke_cert (725ページ)*。
`revoke_non_exist_cert <options>`	ICAが発行した実在しない証明書を取り消します。 参照: *cpca_client revoke_non_exist_cert (728ページ)*。
`search <options>`	ICA内の証明書を検索します。 参照: *cpca_client search (729ページ)*。
`set_ca_services <options>`	認証局サービスポータルを制御します。 参照: *cpca_client set_ca_services (732ページ)*。
`set_cert_validity <options>`	新しい証明書に対するデフォルトの証明書有効期間を設定します。 参照: *cpca_client set_cert_validity (734ページ)*。
`set_mgmt_tool <options>`	ICA管理ツールを制御します。 参照: *cpca_client set_mgmt_tool (735ページ)*。
`set_sign_hash <options>`	CAがファイルハッシュの署名に使用するハッシュアルゴリズムを設定します。 参照: *cpca_client set_sign_hash (740ページ)*。

cpca_client create_cert

説明

Security Management ServerまたはDomain Management Server用のSIC証明書を発行します。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d] create_cert [-p <CA port number>] -n "CN=<Common Name>" -f <Full Path to PKCS12 file> [-w <Password>] [-k {SIC | USER | IKE | ADMIN_PKG}] [-c "<Comment for Certificate>"]
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
`-p <CA port number>`	認証局への接続に使用するSecurity Management ServerまたはDomain Management ServerのTCPポートを指定します。 デフォルトのTCPポート番号は18209です。
`-n "CN=<Common Name>"`	CNを指定された<Common Name>に設定します。
`-f <Full Path to PKCS12 file>`	証明書とキーを格納するPKCS12ファイルを指定します。
`-w <Password>`	オプションです。証明書のパスワードを指定します。
`-k {SIC | USER | IKE | ADMIN_PKG}`	オプションです。証明書の種類を指定します。
`-c "<Comment for Certificate>"`	オプションです。証明書のコメントを指定します(二重引用符で囲む必要があります)。

例

```
[Expert@MGMT:0]# cpca_client create_cert -n "cn=cp_mgmt" -f $CPDIR/conf/sic_cert.p12
```

cpca_client double_sign

説明

証明書の2つ目の署名を作成します。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d] double_sign [-p <CA port number>] -i <Certificate File in PEM format> [-o <Full Path to Output File>]
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
`-p <CA port number>`	オプションです。認証局への接続に使用するSecurity Management ServerまたはDomain Management ServerのTCPポートを指定します。 デフォルトのTCPポート番号は18209です。
`-i <Certificate File in PEM format>`	指定された証明書をインポートします(PEM形式のみ)。
`-o <Full Path to Output File>`	オプションです。証明書を指定したファイルに保存します。

例

```
[Expert@MGMT:0]# cpca_client double_sign -i certificate.pem

 Requesting Double Signature for the following Certificate:
        refCount: 1
        Subject: Email=example@example.com,CN=http://www.example.com/,OU=ValiCert Class 2
Policy Validation Authority,O=exampleO\, Inc.,L=ExampleL Validation Network

 Double Sign of Cert:
 ====================
 (
        : (
                :dn ("Email=example@example.com,CN=http://www.example.com/,OU=exampleOU Class 2
Policy Validation Authority,O=exampleO\, Inc.,L=exampleL Validation Network")
                :doubleSignCert (52016390... ... ...ebb67e96)
                :return_code (0)
        )
)

[Expert@MGMT:0]#
```

cpca_client get_crldp

説明

内部認証局(ICA)に設定された完全修飾ドメイン名(FQDN)を表示します("*cp_conf ca (688 ページ)*"コマンド)。

管理サーバはこのFQDNを使用する:

1. ICAが生成するすべての証明書にCRL DP(Certificate Revocation List Distribution Point)プロパティを設定するには、以下の手順に従います。
2. CRLにアクセスするためのURLを作成

   例:`http://MyMGMT.checkpoint.com:18264/ICA_CRL1.crl`

構文

```
cpca_client [-d] get_crldp [-p <ICA port number>]
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-p <ICA port number>`	オプションです。 認証局への接続に使用するSecurity Management ServerまたはDomain Management ServerのTCPポートを指定します。 デフォルトのTCPポート番号は18264です。

例

```
[Expert@MyMGMT:0]# hostname
MyMGMT
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# domainname
checkpoint.com
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# cpca_client get_crldp
MyMGMT.checkpoint.com
[Expert@MyMGMT:0]
```

cpca_client get_pubkey

説明

ICAの証明書の公開鍵のエンコードをファイルに保存します。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d] get_pubkey [-p <CA port number>] <Full Path to Output File>
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、scriptコマンドを使用してCLIセッション全体を保存してください。
-p <CA port number>	認証局への接続に使用するSecurity Management ServerまたはDomain Management ServerのTCPポートを指定します。 デフォルトのTCPポート番号は18209です。
<Full Path to Output File>	ICAの証明書の公開鍵のエンコードを指定されたファイルに保存します。

例

```
[Expert@MGMT:0]# cpca_client get_pubkey /tmp/key.txt[Expert@MGMT:0]#
[Expert@MGMT:0]# cat /tmp/key.txt
3082010a... ... ...f98b8910
[Expert@MGMT:0]#
```

cpca_client init_certs

説明

ユーザのDN(Distinguished Names) リストをインポートし、各ユーザの登録キーを含むファイルを作成します。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d] init_certs [-p <CA port number>] -i <Full Path to Input File> -o <Full Path to Output File>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-p <CA port number>`	オプションです。認証局への接続に使用するSecurity Management ServerまたはDomain Management ServerのTCPポートを指定します。 デフォルトのTCPポート番号は18209です。

`-i <Full Path to Input File>`	指定されたファイルをインポートします。
	必ずフルパスで入力してください。
	指定したファイルの各DNの間に空行があることを確認します。
	例:
	`...CN=test1,OU=users...`
	`<Empty Line>`
	`...CN=test2,OU=users...`

`-o <Full Path to Output File>`	登録キーを指定されたファイルに保存します。 このコマンドは、エラーメッセージを同じディレクトリにある`<Name of Output File>.failures`ファイルに保存します。

cpca_client lscert

説明

ICAが発行したすべての証明書を表示します。

注：
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d] lscert [-dn <SubString>] [-stat {Pending | Valid
| Revoked | Expired | Renewed}] [-kind {SIC | IKE | User | LDAP}]
[-ser <Certificate Serial Number>] [-dp <Certificate Distribution
Point>]
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-dn <SubString>`	オプションです。指定と一致するDNで検索結果を絞り込む*<SubString>*. このコマンドは、複数の値をサポートしません。
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	オプションです。検索結果を、指定したステータスと一致する証明書のステータスを持つものに絞り込みます。 このコマンドは、複数の値をサポートしません。
`-kind {SIC | IKE | User | LDAP}`	オプションです。検索結果を、指定した種類に一致する証明書の種類を持つものに絞り込みます。 このコマンドは、複数の値をサポートしません。
`-ser <Certificate Serial Number>`	オプションです。検索結果を、指定したシリアル番号と一致する証明書シリアル番号を持つものに絞り込みます。 このコマンドは、複数の値をサポートしません。
`-dp <Certificate Distribution Point>`	オプションです。検索結果を指定したCDP(Certificate Distribution Point) に絞り込みます。 このコマンドは、複数の値をサポートしません。

例

```
[Expert@MGMT:0]# cpca_client lscert -stat Revoked
Operation succeeded. rc=0.
5 certs found.

Subject = CN=VSX2,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 5521   DP = 0
Not_Before: Sun Apr  8 14:10:01 2018   Not_After: Sat Apr  8 14:10:01 2023

Subject = CN=VSX1,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 9113   DP = 0
Not_Before: Sun Apr  8 14:09:02 2018   Not_After: Sat Apr  8 14:09:02 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#


[Expert@MGMT:0]# cpca_client lscert -kind IKE
Operation succeeded. rc=0.
3 certs found.

Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 27214   DP = 1
Not_Before: Wed Apr 11 17:26:02 2018   Not_After: Tue Apr 11 17:26:02 2023

Subject = CN=VSX_Cluster VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 64655   DP = 1
Not_Before: Mon Apr  9 19:36:31 2018   Not_After: Sun Apr  9 19:36:31 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#
```

cpca_client revoke_cert

説明

ICAが発行した証明書を取り消します。

注：
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d] revoke_cert [-p <CA port number>] -n "CN=<Common Name>" -s <Certificate Serial Number>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-p <CA port number>`	オプションです。認証局への接続に使用するSecurity Management ServerまたはDomain Management ServerのTCPポートを指定します。 デフォルトのTCPポート番号は18209です。

`-n "CN=<Common Name>"`	証明書のCNを指定します。
	CNを取得するには*cpca_client lscert (722ページ)*コマンドを実行し、"Subject ="と",O=..."の間に表示されるテキストを確認します。
	例
	この出力から
	`Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x`
	`Status = Valid Kind = IKE Serial = 27214 DP = 1`
	`Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023`
	とすると、このような構文になります。
	`-n "CN=VS1 VPN Certificate`
	注 - パラメータ'-n'のみ、またはパラメータ"-s"と共に使用することができます。

`-s <Certificate Serial Number>`	証明書シリアル番号を指定します。 シリアル番号を確認するには*cpca_client lscert (722ページ)*コマンドを実行します。 **注** -パラメータ"-s"のみ、またはパラメータ"-n"と共に使用することができます。

例 1 - CN で指定された証明書を取り消す場合

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -n "CN=VS1 VPN Certificate"
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

例2 - シリアル番号で指定された証明書を取り消す場合

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -s 27214
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

cpca_client revoke_non_exist_cert

説明

ICAが発行した実在しない証明書を取り消します。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d] revoke_non_exist_cert -i <Full Path to Input File>
```

パラメータ

パラメータ	説明
-d	cpca_clientコマンドをデバッグで実行します。
-i <*Full Path to Input File*>	取り消す証明書のリストを格納したファイルを指定します。 同じ形式で作成する必要があります。*cpca_client lscert (722ページ)*コマンドでの出力表示。 **例** Subject = CN=cp_mgmt,O=MGMT.5p72vp Status = Valid Kind = SIC Serial = 30287 DP = 0 Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023 <Empty Line> Subject = CN=cp_mgmt,O=MGMT.5p72vp Status = Valid Kind = SIC Serial = 60870 DP = 0 Not_Before: Sat Apr 7 19:40:13 2018 Not_After: Fri Apr 7 19:40:13 2023

注 - このコマンドは、エラーメッセージを*<Name of Input File>*.failuresファイルに保存します。

cpca_client search

説明

ICA内の証明書を検索します。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d] search <String> [-where {dn | comment | serial | device_type | device_id | device_name}] [-kind {SIC | IKE | User | LDAP}] [-stat {Pending | Valid | Revoked | Expired | Renewed}] [-max <Maximum Number of Results>] [-showfp {y | n}]
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
<String>	証明書の検索対象テキストを指定します。 入力できる文字列は、スペースを含まない1つの文字列のみです。

パラメータ	説明
`-where {dn | comment | serial | device_type | device_id | device_name}`	オプションです。文字列を検索する、証明書のフィールドを指定します。 ■ `dn`- 証明書DN ■ `comment`- 証明書コメント ■ `serial`- 証明書シリアル番号 ■ `device_type`- デバイスタイプ ■ `device_id`- デバイスID ■ `device_name`- デバイス名 デフォルトでは、すべてのフィールドで検索します。
`-kind {SIC | IKE | User | LDAP}`	オプションです。検索する証明書の種類を指定します。 このフォーマットで複数の値を入力することができます。 `-kind <Kind1> <Kind2> <Kind3>` デフォルトでは、全種類を検索します。
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	オプションです。検索する証明書のステータスを指定します。 このフォーマットで複数の値を入力することができます。 `-stat <Status1> <Status2> <Status3>` デフォルトでは、すべてのステータスを検索します。
`-max <Maximum Number of Results>`	オプションです。結果の表示最大数を指定します。 ■ 範囲：1以上 ■ デフォルト：200
`-showfp {y | n}`	オプションです。証明書のフィンガープリントとサムプリントを表示するかどうかを指定します。 ■ `y`- フィンガープリントとサムプリントを表示（デフォルト） ■ `n`- フィンガープリントとサムプリントを表示しない

例1

```
[Expert@MGMT:0]# cpca_client search samplecompany -where comment -kind SIC LDAP -stat Pending
Valid Renewed
```

例2

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dnOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
Fingerprint = XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX
Thumbprint = xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
[Expert@MGMT:0]#
```

例3

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dn -showfp nOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
[Expert@MGMT:0]#
```

cpca_client set_ca_services

説明

このコマンドは、TCPポート18268のManagement Server上の認証局サービスポータルを有効または無効にします。

このポータルから、該当する内部認証局の証明書をダウンロードすることができます。

信頼のために、該当するSecurity Gateway、外部で管理されているサイト間VPNピアゲートウェイ、リモートアクセスVPNクライアント、クライアントレスVPNを使用するクライアントなどにこの証明書をインストールできます。

注 - R82では、管理サーバのTCPポート18264は、CRL(証明書失効リスト)の検索にのみ使用できます。

構文

```
cpca_client set_ca_services {on | off}
```

パラメータ

パラメータ	説明
on	認証局サービスポータルを有効します
off	認証局サービスポータルを無効にします

Security Management Serverの手順

認証局サービスポータルの有効化

1. セキュリティ管理サーバのコマンドラインに接続します。
2. エキスパートモードにログインします。
3. 認証局サービスポータルを有効化します。

   ```
   cpca_client set_ca_services on
   ```

4. Webブラウザで、次に接続します。

   ```
   http://<IP Address of Security Management Server>:18268
   ```

5. 必要な証明書をダウンロードします。
6. この証明書を該当するコンピュータにインストールします。

認証局サービスポータルの無効化

1. セキュリティ管理サーバのコマンド ラインに接続します。
2. エキスパートモードにログインします。
3. 認証局サービスポータルを無効にします。

```
cpca_client set_ca_services off
```

ドメイン管理サーバの手順

認証局サービスポータルの有効化

1. マルチドメインサーバのコマンドラインに接続します。
2. エキスパートモードにログインします。
3. ドメイン管理サーバのコンテキストに移動します。

```
mdsenv <IP Address or Name of Domain Management Server>
```

4. 認証局サービスポータルを有効化します。

```
cpca_client set_ca_services on
```

5. Webブラウザで、次に接続します。

```
http://<IP Address of Domain Management Server>:18268
```

6. 必要な証明書をダウンロードします。
7. この証明書を該当するコンピュータにインストールします。

認証局サービスポータルの無効化

1. マルチドメインサーバのコマンドラインに接続します。
2. エキスパートモードにログインします。
3. ドメイン管理サーバのコンテキストに移動します。

```
mdsenv <IP Address or Name of Domain Management Server>
```

4. 認証局サービスポータルを無効にします。

```
cpca_client set_ca_services off
```

cpca_client set_cert_validity

説明

このコマンドは、新しい証明書に対するデフォルトの証明書有効期間を設定します。

注:

- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- 新しい証明書の有効期限は、この変更後に作成する証明書にのみ適用されます。

構文

```
cpca_client set_cert_validity -k {SIC | IKE | USER} [-y <Number of Years>] [-d <Number of Days>] [-h <Number of Hours>] [-s <Number of Seconds>]
```

パラメータ

パラメータ	説明
`-k {SIC | IKE | USER}`	証明書の種類を指定します。
`-y <Number of Years>`	有効期限(年単位)を指定します。
`-d <Number of Days>`	有効期限(日数)を指定します。
`-h <Number of Hours>`	有効期限(時間単位)を指定します。
`-s <Number of Seconds>`	有効期限(秒単位)を指定します。

例

```
[Expert@MGMT:0]# cpca_client set_cert_validity -k IKE -y 3
 cert validity period was changed successfully.
[Expert@MGMT:0]#
```

cpca_client set_mgmt_tool

説明

ICA管理ツールを制御します。

このツールは、デフォルトでは無効です。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

参照: sk102837: Best Practices - ICA Management Tool configuration

構文

```
cpca_client [-d] set_mgmt_tool {on | off | add | remove | clean |
print} [-p <CA port number>] [{-a <Administrator DN> | -u <User
DN> | -c <Custom User DN>}]
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、scriptコマンドを使用してCLIセッション全体を保存してください。
on	ICA管理ツールを起動します。
off	ICA管理ツールを停止します。
add	ICA管理ツールの使用を許可された、指定された管理者、ユーザ、またはカスタムユーザを追加します。
remove	ICA管理ツールの使用を許可されている、指定された管理者、ユーザ、またはカスタムユーザを削除します。
clean	ICA管理ツールの使用を許可されているすべての管理者、ユーザ、またはカスタムユーザを削除します。
print	ICA管理ツールの使用を許可する、設定された管理者、ユーザ、またはカスタムユーザが表示されます。

パラメータ	説明
`-p <CA port number>`	オプションです。認証局への接続に使用するSecurity Management ServerまたはDomain Management ServerのTCPポートを指定します。 デフォルトのTCPポート番号は18265です。
`-a <Administrator DN>`	オプションです。ICA管理ツールの使用を許可された管理者のDNを指定します。 SmartConsoleに表示される完全なDNを指定する必要があります。 **手順** 1. **Object Explorer** > を開く**Users** 2. Administratorオブジェクトまたは**User**オブジェクトのプロパティを開きます。 3. **Certificates**ペインをクリックします。 4. 証明書を選択し、鉛筆アイコンをクリックします。 5. クリック**View certificate details** 6. **Certificate Info**ウィンドウで、**Details**タブをクリックします。 7. **Subject**フィールドをクリックします。 8. すべてのフィールドを連結します 例: `-a "CN=ICA_Tool_Admin,OU=users,O=MGMT.s6t98x"`
`-u <User DN>`	オプションです。ICA管理ツールの使用を許可されたユーザのDNを指定します。 SmartConsoleに表示される完全なDNを指定する必要があります。 **手順** 1. **Object Explorer** > を開く**Users** 2. Administratorオブジェクトまたは**User**オブジェクトのプロパティを開きます。 3. **Certificates**ペインをクリックします。 4. 証明書を選択し、鉛筆アイコンをクリックします。 5. クリック**View certificate details** 6. **Certificate Info**ウィンドウで、**Details**タブをクリックします。 7. **Subject**フィールドをクリックします。 8. すべてのフィールドを連結します 例: `-u "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

パラメータ	説明
`-c <Custom User DN>`	オプションです。ICA管理ツールの使用を許可されたカスタムユーザのDNを指定します。 SmartConsoleに表示される完全なDNを指定する必要があります。 **手順** 1. **Object Explorer** >を開く**Users** 2. Administratorオブジェクトまたは**User**オブジェクトのプロパティを開きます。 3. **Certificates**ペインをクリックします。 4. 証明書を選択し、鉛筆アイコンをクリックします。 5. クリック**View certificate details** 6. **Certificate Info**ウィンドウで、**Details**タブをクリックします。 7. **Subject**フィールドをクリックします。 8. すべてのフィールドを連結します 例: `-c "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

注 - パラメータ"`-a`"または"`-u`"を指定せずに"`cpca_client set_mgmt_tool`"コマンドを実行した場合、許可された管理者とユーザのリストは変更されません。あらかじめ定義された許可された管理者およびユーザが、ICA管理ツールを起動および停止することができます。

ICA管理ツールに接続するには

1. SmartConsoleで、必要な管理者オブジェクトとユーザオブジェクトを設定します。

   これらの管理者とユーザのために証明書を作成する必要があります。

   この証明書を使用して、ICA管理ツールおよびクライアントのWebブラウザで許可ユーザを設定します。

2. 管理サーバのコマンドラインで、ICA管理ツールの使用を許可する管理者とユーザを追加します。

   ```
   cpca_client set_mgmt_tool add ...
   ```

3. 管理サーバのコマンドラインで、ICA管理ツールを起動します。

   ```
   cpca_client set_mgmt_tool on
   ```

4. ICA管理ツールのステータスを確認します:

   ```
   cpca_client set_mgmt_tool print
   ```

5. 管理者/ユーザの証明書をWindows証明書ストアにインポート:

   a. 必要な管理者 / ユーザを作成した際に保存した*.p12 ファイルを右クリックし、**Install PFX**をクリックします。

      Certificate Import Wizardが開きます。

   b. **Store Location**セクションで、該当するオプションを選択します:

      - **Current User**(デフォルト)
      - **Local Machine**

   c. クリック**Next**。

   d. 必要な管理者/ユーザ証明書を作成したときに使用したのと同じ証明書パスワードを入力します。

   e. **Enable strong private key protection**をクリアします。

   f. **Mark this key as exportable**を選択します。

   g. クリック**Next**。

   h. **Place all certificates in the following store**を選択 > **Browse**をクリック > **Personal**を選択 > **OK**をクリックします。

   i. クリック**Next**。

   j. クリック**Finish**。

6. Webブラウザで**ICA管理ツール**に接続します:

   ```
   https://<IP Address of the Management Server>:18265
   ```

   重要 - TCPポート18265が開いていることは脆弱性ではありません。ICA管理ツールポータルはSSLで保護されています。さらに、証明書を使用してアクセスできるのは、権限を持つ管理者とユーザのみです。

7. このメッセージのダイアログボックスが表示されます:

   ```
   Client Authentication

   Identification

   The Web site you want to view requests identification.

   Select the certificate to use when connecting.
   ```

8. **ICA管理ツール**の認証に適した証明書を選択します。
9. **OK**をクリックします。
10. **Security Alert**ダイアログボックスで、**Yes**をクリックします。

cpca_client set_sign_hash

説明

CAがファイルハッシュの署名に使用するハッシュアルゴリズムを設定します。sk103840も参照。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_client [-d] set_sign_hash {sha1 | sha256 | sha384 | sha512}
```

重要 - この変更後は、次のコマンドを使用してCheck Pointのサービスを再起動する必要があります:

- Security Management Serverで次を実行します:
  1. `cpstop`
  2. `cpstart`
- マルチドメインサーバで次を実行します:
  1. `mdsstop_customer <Name or IP Address of Domain Management Server>`
  2. `mdsstart_customer <Name or IP Address of Domain Management Server>`

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script` コマンドを使用してCLIセッション全体を保存してください。
`{sha1 | sha256 | sha384 | sha512}`	CAがファイルハッシュを署名するために使用するハッシュアルゴリズム。 デフォルトのアルゴリズムはSHA-256です。

例

```
[Expert@MGMT:0]# cpca_client set_sign_hash sha256

You have selected the signature hash function SHA-256
WARNING: This hash algorithm is not supported in Check Point gateways prior to R71.
WARNING: It is also not supported on older clients and SG80 R71.

Are you sure? (y/n)
y
Internal CA signature hash changed successfully.
Note that the signature on the Internal CA certificate has not changed, but this has no
security implications.
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpstop ; cpstart
```

cpca_create

説明

Check Point内部認証局 (ICA) データベースを新しく作成します。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cpca_create [-d] -dn <CA DN>
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
-dn <CA DN>	認証局識別名 (DN) を指定します。

cpconfig

説明

このコマンドは、Check Point Configuration Toolを起動します。

このユーティリティは、インストールされているCheck Point製品の特定の設定を行うものです。

構文

```
cpconfig
```

注 - マルチドメインサーバでは"`mdsconfig`"コマンドを実行します。

メニューオプション

注 - 表示されるオプションは、設定およびインストールされている製品によって異なります。

メニューオプション	説明
Licenses and contracts	このサーバにおけるCheck Pointのライセンスとコントラクトを管理します。
Administrator	このサーバにCheck Pointのシステム管理者を設定します。
GUI Clients	SmartConsoleを使用して、このサーバに接続できるGUIクライアントを設定します。
SNMP Extension	利用不可。このオプションは使用**しないで**ください。 SNMPを設定するには*R82 Gaia Administration Guide*- 章「*システム管理*」- セクション*SNMP*
Random Pool	Gaiaオペレーティングシステムで使用するRSA鍵を設定します。
Certificate Authority	内部認証局(ICA)を初期化し、認証局(CA)の完全修飾ドメイン名(FQDN)を設定します。
Certificate's Fingerprint	ICAのフィンガープリントを表示します。 このフィンガープリントは、サーバのICA証明書から取得したテキスト文字列です。 このフィンガープリントは、SmartConsoleでサーバに接続する際に、サーバの識別を確認するものです。
Automatic start of Check Point Products	インストールされているCheck Point製品のうち、起動時に自動的に起動する製品を表示および制御します。
Exit	Check Point Configuration Toolを終了します。

例 - Security Management Server上のメニュー

```
[Expert@MyMGMT:0]# cpconfig
This program will let you re-configure
your Check Point Security Management Server configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) Administrator
(3) GUI Clients
(4) SNMP Extension
(5) Random Pool
(6) Certificate Authority
(7) Certificate's Fingerprint
(8) Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :
```

cpinfo

説明

実行時にCheck Pointコンピュータの診断データを収集するユーティリティです。

これらのデータを収集することは、Check Pointサーバの問題について問い合わせる際に*Check Point Support*必要となっています。

詳細は、sk92739を参照してください。

Cplic

説明

`cplic`コマンドは、Check Pointのライセンスを管理するコマンドです。

このコマンドは、Gaia Clishまたはエキスパートモードで実行できます。

ライセンス管理は、3種類のコマンドに分かれています。

ライセンスコマンド	適用先	説明
ローカルライセンスコマンド	管理サーバ、セキュリティゲートウェイとクラスタメンバ	これらのコマンドは、Check Pointのコンピュータでローカルに実行します。
リモートライセンスコマンド	管理サーバのみ	Security Management ServerまたはDomain Management Serverでこれらのコマンドを実行します。これらの変更は、管理されたセキュリティゲートウェイとクラスタメンバに影響します。
ライセンスリポジトリコマンド	管理サーバのみ	Security Management ServerまたはDomain Management Serverでこれらのコマンドを実行します。これらの変更は、ローカルライセンスリポジトリに保存されているライセンスに影響します。

Management Server本体でローカルライセンスを行うための構文

```
cplic [-d]
      {-h | -help}
      check <options>
      contract <options>
      del <options>
      print <options>
      put <options>
```

管理下のセキュリティゲートウェイとクラスタメンバでリモートライセンスを行うための構文

```
cplic [-d]
      {-h | -help}
      del <options>
      get <options>
      put <options>
      upgrade <options>
```

Management Serverのライセンスデータベース操作の構文

```
cplic [-d]
      {-h | -help}
      db_add <options>
      db_print <options>
      db_rm <options>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`{-h | -help}`	該当する組み込みの使用状況を表示します。
`check <options>`	ライセンスにローカルSecurity GatewayまたはManagement Server上の機能が含まれていることを確認します。 参照: *cplic check (750ページ)*。
`contract <options>`	ローカルのCheck Pointコンピュータ上のCheck Pointサービスコントラクトを管理(削除およびインストール)します。 参照: *cplic contract (752ページ)*。
`db_add <options>`	管理サーバにのみ適用されます。 管理サーバのライセンスリポジトリにライセンスを追加します。 参照: *cplic db_add (754ページ)*。

パラメータ	説明
`db_print <options>`	管理サーバにのみ適用されます。 管理サーバのライセンスリポジトリに保存されているCheck Pointライセンスの詳細が表示されます。 参照: *cplic db_print (756ページ)*。
`db_rm <options>`	管理サーバにのみ適用されます。 Management Server上のライセンスリポジトリからライセンスを削除します。 参照: *cplic db_rm (758ページ)*。
`del <options>`	不要な評価版ライセンス、期限切れライセンス、その他のライセンスを含む、ホスト上のCheck Pointライセンスを削除します。 参照: *cplic del (759ページ)*。
`del <Object Name> <options>`	リモート管理されたセキュリティゲートウェイまたはクラスタメンバからセントラルライセンスをデタッチします。 参照: *cplic del <object name> (760ページ)*。
`get <options>`	管理サーバにのみ適用されます。 管理しているSecurity Gatewayとクラスタメンバから、Management Server上のライセンスリポジトリにすべてのライセンスを取り込みます。 参照: *cplic get (761ページ)*。
`print <options>`	ローカルのCheck Pointコンピュータにインストールされているライセンスの詳細を出力します。 参照: *cplic print (763ページ)*。
`put <options>`	Check Pointのコンピュータにライセンスをインストールし、アタッチします。 参照: *cplic put (765ページ)*。
`put <Object Name> <options>`	リモート管理されたセキュリティゲートウェイとクラスタメンバに、1つまたは複数のセントラルライセンスまたはローカルライセンスをアタッチします。 参照: *cplic put <object name> (768ページ)*。
`upgrade <options>`	管理サーバにのみ適用されます。 ライセンスリポジトリのライセンスを、指定されたライセンスファイルのライセンスでアップグレードします。 参照: *cplic upgrade (771ページ)*。

cplic check

説明

ライセンスにローカルSecurity GatewayまたはManagement Server上の機能が含まれていることを確認します。sk66245を参照してください。

構文

```
cplic check {-h | -help}
```

```
cplic [-d] check [-p <Product>] [-v <Version>] [{-c | -count}] [-t <Date>] [{-r | -routers}] [{-S | -SRusers}] <Feature>
```

実行できるコマンド:

- Gaia ClishまたはエキスパートモードのManagement Server / Security Gateway / Cluster Member上
- Gaia gClishまたはエキスパートモードのScalable Platform Security Group

パラメータ

パラメータ	説明
`{-h | -help}`	該当する組み込みの使用状況を表示します。
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-p <Product>`	ライセンス情報を要求される製品。 製品の一例: ■ `fw1` - セキュリティゲートウェイ/クラスタメンバ/セキュリティグループ(すべてのSoftware Blade)、または管理サーバ(すべてのSoftware Blade)のFireWall-1インフラストラクチャ ■ `mgmt` - マルチドメインサーバインフラストラクチャ ■ `services` - 各種サービスの資格 ■ `cvpn` - モバイルアクセス ■ `etm` - QoS (FloodGate-1) ■ `eps` - 管理サーバ上のEndpoint Software Blades

パラメータ	説明
-v <*Version*>	ライセンス情報を要求する製品のバージョン。
{-c | -count}	この機能に接続されているライセンス数を出力します。
-t <*Date*>	未来の日付でライセンス状況を確認します。 **ddmmyyyy**の形式を使用します。 特定の日付において、あるライセンスでは有効な機能が、別のライセンスでは無効となる場合があります。
{-r | -routers}	ルータがいくつまで許容されるかを確認します。 <*Feature*>オプションは必要ありません。
{-S | -SRusers}	許可するSecuRemoteユーザの数を確認します。
<*Feature*>	ライセンス情報を要求される機能。

管理サーバからの例

```
[Expert@MGMT]# cplic print -p
Host Expiration Primitive-Features
W.X.Y.Z 24Mar2016 ::CK-XXXXXXXXXXX fw1:6.0:swb fw1:6.0:comp fw1:6.0:compunlimited fw1:6.0:cluster-1 fw1:6.0:cpxmgmt_qos_u_sites
fw1:6.0:sprounl fw1:6.0:nxunlimit fw1:6.0:swp evnt:6.0:smrt_evnt fw1:6.0:fwc fw1:6.0:ca fw1:6.0:rtmui fw1:6.0:sstui fw1:6.0:fwlv
fw1:6.0:cmd evnt:6.0:alzd5 evnt:6.0:alzc1 evnt:6.0:alzs1 fw1:6.0:sstui fw1:6.0:fwlv fw1:6.0:sme10 etm:6.0:rtm_u fw1:6.0:cep1 fw1:6.0:rt
fw1:6.0:cemid fw1:6.0:web_sec_u fw1:6.0:workflow fw1:6.0:ram1 fw1:6.0:routers fw1:6.0:supmgmt fw1:6.0:supunlimit fw1:6.0:prov
fw1:6.0:atlas-unlimit fw1:6.0:filter fw1:6.0:ui psmp:6.0:psmsunlimited fw1:6.0:vpe_unlimit fw1:6.0:cluster-u fw1:6.0:remote1 fw1:6.0:aes
fw1:6.0:strong fw1:6.0:rdp fw1:6.0:des fw1:6.0:isakmp fw1:6.0:dbvr_unlimit fw1:6.0:cmpmgmt fw1:6.0:rtmmgmt fw1:6.0:fgmgmt fw1:6.0:blades
fw1:6.0:cpipv6 fw1:6.0:mgmtha fw1:6.0:remote
[Expert@MGMT]#
```

ハイアベイラビリティの管理サーバからの例

```
[Expert@MGMT]# cplic check -p fw1 -v 6.0 -c mgmtha
cplic check 'mgmtha': 1 licenses
[Expert@MGMT]#
```

cplic contract

説明

ローカルのCheck Pointコンピュータ上のCheck Point Service Contractを削除します。

ローカルのCheck PointコンピュータにCheck Point Service Contractをインストールします。

注意

- Service Contractファイルの詳細：sk33089: What is a Service Contract File?
- 管理対象のセキュリティゲートウェイ/クラスタメンバ/Scalable Platformセキュリティグループにサービスコントラクトをインストールする場合は、該当する管理サーバのアプリケーションライセンスリポジトリを更新する必要があります。*cplic get (761ページ)*コマンド、またはSmartUpdate。

構文

```
cplic contract -h
```

```
cplic [-d] contract
      del
            -h
            <Service Contract ID>
      put
            -h
            [{-o | -overwrite}] <Service Contract File>
```

実行できるコマンド：

- Gaia ClishまたはエキスパートモードのManagement Server / Security Gateway / Cluster Member上
- Gaia gClishまたはエキスパートモードのScalable Platform Security Group

パラメータ

パラメータ	説明
`{-h | -help}`	該当する組み込みの使用状況を表示します。
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`del`	ローカルのCheck Pointコンピュータ上の`$CPDIR/conf/cp.contract`ファイルからサービスコントラクトを削除します。
`put`	サービスコントラクトをローカルのCheck Pointコンピュータ上の`$CPDIR/conf/cp.contract`ファイルにマージします。
<Service Contract ID>	サービスコントラクトのID。
`{-o | -overwrite}`	現在のサービスコントラクトを上書きすることを指定します。
<Service Contract File>	サービスコントラクトのファイルへのパスとファイル名。 まず、サービスコントラクトファイルを次からダウンロードします: *Check Point User Center*アカウント

cplic db_add

説明

管理サーバのライセンスリポジトリにライセンスを追加します。

ライセンスリポジトリにローカルライセンスを追加すると、Management Serverは、一致するIPアドレスを持つ管理されたSecurity Gateway / Cluster Memberに自動的にライセンスをアタッチします。

セントラルライセンスを追加する場合、手動でアタッチする必要があります。

注 - ライセンスの詳細は*Check Point User Center*。

構文

```
cplic db_add {-h | -help}
```

```
cplic [-d] db_add -l <License File> [<Host>] [<Expiration Date>]
[<Signature>] [<SKU/Features>]
```

パラメータ

パラメータ	説明
`{-h | -help}`	該当する組み込みの使用状況を表示します。
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-l <License File>`	ライセンスを格納したファイルの名前。
<Host>	Security Management Server / Domain Management Server のホスト名またはIPアドレス。
<Expiration Date>	ライセンスの有効期限。
<Signature>	ライセンス署名の文字列。 例：`aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` 大文字と小文字を区別します。ハイフンは省略可能です。

パラメータ	説明
<*SKU/Features*>	ライセンスのSKUには、ライセンスに含まれる機能がまとめられています。 たとえば`CPSUITE-EVAL-3DES-vNG`

例

ファイル`192.0.2.11.lic`に1つ以上のライセンスが含まれている場合、コマンド "`cplic db_add -l 192.0.2.11.lic`" は次のような出力を生成します。

```
[Expert@MGMT]# cplic db_add -l 192.0.2.11.lic
Adding license to database ...
Operation Done
[Expert@MGMT]#
```

cplic db_print

説明

管理サーバのライセンスリポジトリに保存されているCheck Pointライセンスの詳細が表示されます。

構文

```
cplic db_print {-h | -help}
```

```
cplic [-d] db_print {<Object Name> | -all} [{-n | -noheader}] [-x]
[{-t | -type}] [{-a | -attached}]
```

パラメータ

パラメータ	説明
{-h | -help}	該当する組み込みの使用状況を表示します。
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
<Object Name>	<Object Name>に添付されたライセンスのみを出力します。 <Object Name>は、SmartConsoleで定義されているセキュリティゲートウェイ / クラスタメンバオブジェクトの名前です。
-all	ライセンスリポジトリにあるすべてのライセンスを出力します。
{-n | -noheader}	ヘッダなしのライセンスを出力します。
-x	署名入りライセンスを出力します。
{-t | -type}	ライセンスの種類を表示：セントラルまたはローカル
{-a | -attached}	ライセンスがどのオブジェクトにアタッチされているかを示します。 パラメータ"-all"が指定されている場合に有効です。

例

```
[Expert@MGMT:0]# cplic db_print -all
 Retrieving license information from database ...

The following licenses appear in the database:
==============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXX
[Expert@MGMT:0]#

[Expert@MGMT:0]# cplic db_print -all -x -a
 Retrieving license information from database ...

The following licenses appear in the database:
==============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXX  MGMT
[Expert@MGMT:0]#
```

cplic db_rm

説明

Management Server上のライセンスリポジトリからライセンスを削除します。

リポジトリからライセンスを削除した後は、そのライセンスを使用することができなくなります。

警告 - このコマンドを実行できるのは、次のコマンドでライセンスを切り離した後だけです。
*cplic del (759ページ)*コマンドを実行します。

構文

```
cplic db_rm {-h | -help}
cplic [-d] db_rm <Signature>
```

パラメータ

パラメータ	説明
{-h | -help}	該当する組み込みの使用状況を表示します。
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
<*Signature*>	ライセンス内の署名文字列。 ライセンスのシグネチャ文字列を見るには*cplic print (763ページ)*コマンドを実行します。

例

```
[Expert@MGMT:0]# cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn
```

cplic del

説明

不要な評価版ライセンス、期限切れライセンス、その他のライセンスを含む、ホスト上のCheck Pointライセンスを削除します。

このコマンドは、ローカルコンピュータとリモート管理コンピュータの両方でライセンスを削除することができます。

構文

```
cplic del {-h | -help}
cplic [-d] del [-F <Output File>] <Signature> <Object Name>
```

実行できるコマンド:

- Gaia ClishまたはエキスパートモードのManagement Server / Security Gateway / Cluster Member上
- Gaia gClishまたはエキスパートモードのScalable Platform Security Group

パラメータ

パラメータ	説明
`{-h | -help}`	該当する組み込みの使用状況を表示します。
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-F <Output File>`	コマンド出力を指定されたファイルに保存します。
`<Signature>`	ライセンス内の署名文字列。 ライセンスのシグネチャ文字列を見るには*cplic print (763ページ)*コマンドを実行します。
`<Object Name>`	SmartConsoleで設定されたSecurity Gateway / クラスタメンバオブジェクトの名前。

cplic del <object name>

説明

リモート管理されたセキュリティゲートウェイまたはクラスタメンバからセントラルライセンスをデタッチします。

このコマンドを実行すると、自動的にライセンスリポジトリが更新されます。

セントラルライセンスは、未アタッチライセンスとしてライセンスリポジトリに残ります。

構文

```
cplic del {-h | -help}
```

```
cplic [-d] del <Object Name> [-F <Output File>] [-ip <Dynamic IP Address>] <Signature>
```

パラメータ

パラメータ	説明
{-h | -help}	該当する組み込みの使用状況を表示します。
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
<Object Name>	SmartConsoleで定義されているSecurity Gateway / クラスタメンバオブジェクトの名前です。
-F <Output File>	コマンド出力を指定されたファイルに保存します。
-ip <Dynamic IP Address>	指定したIPアドレスのDAIP Security Gatewayのライセンスを削除します。 **注** - このパラメータを使用する場合、オブジェクト名はDAIPセキュリティゲートウェイでなければなりません。
<Signature>	ライセンス内の署名文字列。 ライセンスのシグネチャ文字列を見るには*cplic print (763ページ)*コマンドを実行します。

cplic get

説明

管理しているSecurity Gatewayとクラスタメンバから、Management Server上のライセンスリポジトリにすべてのライセンスを取り込みます。

このコマンドは、管理されたSecurity Gatewayとクラスタメンバとライセンスリポジトリを同期させるのに役立ちます。

このコマンドを実行すると、ローカルでのすべての変更でライセンスリポジトリが更新されます。

構文

```
cplic get {-h | -help}
```

```
cplic [-d] get
      -all
      <IP Address>
      <Host Name>
```

パラメータ

パラメータ	説明
{-h | -help}	該当する組み込みの使用状況を表示します。
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
-all	管理されたネットワーク内のすべてのセキュリティゲートウェイとクラスタメンバからライセンスを取得します。
<IP Address>	ライセンスを取得するSecurity Gateway / クラスタメンバのIPアドレス。
<Host Name>	SmartConsoleで定義された、ライセンスを取得するセキュリティゲートウェイ/クラスタメンバーオブジェクトの名前です。

例

オブジェクト名 `MyGW` のSecurity Gatewayに4つのLocalライセンスがあり、ライセンスリポジトリに他の2つのLocalライセンスがある場合、コマンド "`cplic get MyGW`" は次のような出力を生成します。

```
[Expert@MGMT:0]# cplic get MyGW
Get retrieved 4 licenses.
Get removed 2 licenses.
[Expert@MGMT:0]#
```

cplic print

説明

ローカルのCheck Pointコンピュータにインストールされ ているCheck Pointライセンスの詳 細を出 力し ます。

注 - Security Gateway / クラスタメンバ / Scalable Platform Security Groupでは、このコマンドはインストールされているすべてのライセンス(LocalとCentralの両 方) を表 示します。

構文

```
cplic print {-h | -help}
```

```
cplic [-d] print[{-n | -noheader}] [-x] [{-t | -type}] [-F <Output File>] [{-p | -preatures}] [-D]
```

実 行 できるコマンド:

- Gaia ClishまたはエキスパートモードのManagement Server / Security Gateway / Cluster Member上
- Gaia gClishまたはエキスパートモードのScalable Platform Security Group

パラメータ

パラメータ	説明
{-h | -help}	該当する組み込みの使用状況を表示します。
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、scriptコマンドを使用してCLIセッション全体を保存してください。
{-n | -noheader}	ヘッダなしのライセンスを出力します。
-x	署名されたライセンスを出力します。
{-t | -type]	ライセンスの種類を表示します(セントラルまたはローカル) 。
-F <Output File>	コマンド出力を指定されたファイルに保存します。
{-p | -preatures}	プリミティブな機能に解決されたライセンスを出力します。
-D	Multi-Domain Serverでは、ドメインライセンスのみが表示されます。

例1

```
[Expert@HostName:0]# cplic print
Host             Expiration   Features
192.168.3.28     25Aug2019    CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

例2

```
[Expert@HostName:0]# cplic print -x
Host             Expiration   Signature                          Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

cplic put

説明

Check Pointコンピュータに1つまたは複数のローカルライセンスをインストールします。

注 - ライセンスの詳細は*Check Point User Center*。

構文

```
cplic put {-h | -help}
```

```
cplic [-d] put [{-o | -overwrite}] [{-c | -check-only}] [{-s | -select}] [-F <Output File>] [{-P | -Pre-boot}] [{-k | -kernel-only}] -l <License File> [<Host>] [<Expiration Date>] [<Signature>] [<SKU/Features>]
```

実行できるコマンド:

- Gaia ClishまたはエキスパートモードのManagement Server / Security Gateway / Cluster Member上
- Gaia gClishまたはエキスパートモードのScalable Platform Security Group

パラメータ

パラメータ	説明
{-h | -help}	該当する組み込みの使用状況を表示します。
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、scriptコマンドを使用してCLIセッション全体を保存してください。
{-o | -overwrite}	Security Gateway / クラスタメンバ / Scalable Platform Security Groupでは、このコマンドはローカルライセンスのみを消去し、リモートでインストールされているセントラルライセンスは消去しません。
{-c | -check-only}	ライセンスを確認します。ライセンスのIPがCheck Pointコンピュータと一致するかどうか、また署名が有効であるかどうかを確認します。
{-s | -select}	IPアドレスがCheck PointコンピュータのIPアドレスと一致するローカルライセンスのみを選択します。

パラメータ	説明
`-F <Output File>`	コマンド出力を指定されたファイルに保存します。
`{-P | -Pre-boot}`	このオプションは、アップグレード後、Check Pointコンピュータを再起動する前に使用します。 このオプションを使用すると、特定のエラーメッセージが表示されなくなります。
`{-K | -kernel-only}`	現在有効なライセンスをカーネルにプッシュします。 Check Pointサポートのみ使用可能です。
`-l <License File>`	ライセンスを格納したファイルの名前。
`<Host>`	ローカルライセンスのSecurity Gateway / クラスタメンバ / Scalable Platform Security Groupのホスト名またはIPアドレスです。 セントラルライセンスのSecurity Management Server / Domain Management Serverのホスト名またはIPアドレス。
`<Expiration Date>`	ライセンスの有効期限。
`<Signature>`	ライセンス内の署名文字列。 大文字と小文字を区別します。ハイフンは省略可能です。
`<SKU/Features>`	ライセンスのSKUには、ライセンスに含まれる機能がまとめられています。 例：`CPSUITE-EVAL-3DES-vNG`

ユーザセンターから受け取ったライセンスからパラメータをコピーして貼り付けます。

パラメータ	説明
`host`	外部インタフェースのIPアドレス(クワッドドット表記) 。 最後の部分は0または255にすることはできません。
`expiration date`	ライセンスの有効期限。`never`にすることも可能です。
`signature`	ライセンス署名の文字列。 大文字と小文字を区別します。ハイフンは省略可能です。
`SKU/features`	ライセンスのSKUと認証キーを列挙した文字列。 ライセンスのSKUには、ライセンスに含まれる機能がまとめられています。 例：`CPSB-SWB CPSB-ADNC-M CK0123456789ab`

例

```
[Expert@HostName:0]# cplic put -l License.lic
Host Expiration SKU
192.168.2.3 14Jan2016  CPSB-SWB CPSB-ADNC-M CK0123456789ab
[Expert@HostName:0]#
```

cplic put <object name>

説明

リモート管理されたセキュリティゲートウェイとクラスタメンバに、1つまたは複数のセントラルライセンスまたはローカルライセンスをアタッチします。

このコマンドを実行すると、自動的にライセンスリポジトリが更新されます。

注意

- ライセンスの詳細は*Check Point User Center*。
- 複数のライセンスをアタッチできます。

構文

```
cplic put {-h | -help}
```

```
cplic [-d] put <Object Name> [-ip<ダイナミックIPアドレス>] [-F <Output File>] -l <License File> [<Host>] [<Expiration Date>] [<Signature>] [<SKU/Feature>]
```

パラメータ

パラメータ	説明
`{-h | -help}`	該当する組み込みの使用状況を表示します。
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
<Object Name>	SmartConsoleで定義されている、セキュリティゲートウェイ/クラスタメンバオブジェクトの名前です。
`-ip` *<Dynamic IP Address>*	指定したIPアドレスのSecurity Gatewayにライセンスをインストールします。 このパラメータは、動的に割り当てられたIPアドレス(DAIP) を持つSecurity Gatewayにライセンスをインストールするために使用されます。 **注** - このパラメータを使用する場合、オブジェクト名はDAIPセキュリティゲートウェイのものでなければなりません。
`-F` *<Output File>*	コマンド出力を指定されたファイルに保存します。
`-l` *<License File>*	*<ライセンスファイル>*からライセンスをインストールします。
<Host>	Security Management Server / Domain Management Server のホスト名またはIPアドレス。
<Expiration Date>	ライセンスの有効期限。
<Signature>	ライセンス署名の文字列。 大文字と小文字を区別します。ハイフンは省略可能です。
<SKU/Features>	ライセンスのSKUには、ライセンスに含まれる機能がまとめられています。 例：`CPSUITE-EVAL-3DES-vNG`

ユーザセンターから受け取ったライセンスからパラメータをコピーして貼り付けます。

パラメータ	説明
host	外部インタフェースのIPアドレス(クワッドドット表記)。 最後の部分は0または255にすることはできません。
expiration date	ライセンスの有効期限。neverにすることも可能です。
signature	ライセンス署名の文字列。 大文字と小文字を区別します。ハイフンは省略可能です。
SKU/features	ライセンスのSKUと認証キーを列挙した文字列。 ライセンスのSKUには、ライセンスに含まれる機能がまとめられています。 例:CPSB-SWB CPSB-ADNC-M CK0123456789ab

cplic upgrade

説明

ライセンスリポジトリのライセンスを、指定されたライセンスファイルのライセンスでアップグレードします。

注 - このライセンスファイルは*Check Point User Center*。

構文

```
cplic upgrade {-h | -help}
cplic [-d] upgrade -l <Input File>
```

パラメータ

パラメータ	説明
`{-h | -help}`	該当する組み込みの使用状況を表示します。
`-l <Input File>`	ライセンスリポジトリおよびCheck Point Security Gateways /クラスタメンバ内のライセンスを、指定されたファイル内のライセンスと一致するようにアップグレードします。

例

この例では、ライセンスリポジトリのライセンスをアップグレードする手順を説明します。

入力ファイルには、Software Bladeのライセンスが2つあります。

- 1つのライセンスが、リモート管理されたSecurity Gatewayのどのライセンスとも一致しません。
- もう1つのライセンスは、アップグレードが必要な管理されたSecurity Gateway上のNGXバージョンのライセンスと一致します。

この例でのワークフロー:

1. Security Management Serverを最新バージョンにアップグレードします。

   前のバージョンの製品で、Security Management ServerとSecurity Gatewayの間に接続があることを確認します。

2. ライセンスリポジトリにすべてのライセンスをインポートします。

   リモートのSecurity Gatewayの製品をアップグレードした後でも実行できます。

3. このコマンドを実行します。

```
cplic get -all
```

例:

```
[Expert@MyMGMT]# cplic get -all
Getting licenses from all modules ...
MyGW:
Retrieved 1 licenses
```

4. リポジトリ内のすべてのライセンスを確認するには、次のコマンドを実行します。

```
cplic db_print -all -a
```

例:

```
[Expert@MyMGMT]# cplic db_print -all -a
Retrieving license information from database ...

The following licenses appear in the database:
==============================================
Host Expiration Features
192.0.2.11 Never CPFW-FIG-25-53 CK49C3A3CC7121 MyGW1
192.0.2.11 26Nov2017 CPSB-SWB CPSB-ADNC-M CK0123456789ab MyGW2
```

5. .*Check Point User Center*バージョンNGXからSoftware Bladesライセンスにアップグレードされた製品のライセンスを表示します。

   アップグレードライセンスを新規に作成することも可能です。

6. アップグレードライセンスを含むファイルをダウンロードします。

   バージョンNGXからSoftware Bladeにバージョンアップした製品のライセンスのみダウンロードしてください。

7. バージョンNGXのライセンスをリポジトリにインポートしていない場合、このタイミングでバージョンNGXのライセンスをインポートします。

   次のコマンドを実行します。

```
cplic get -all
```

8. ライセンスのアップグレードコマンドを実行します。

```
cplic upgrade -l <Input File>
```

   - ダウンロードしたライセンスファイルとライセンスリポジトリにあるライセンスを比較します。
   - 証明書キーと機能が一致した場合、リポジトリとリモートSecurity Gatewayの古いライセンスが新しいライセンスに更新されます。
   - ライセンスアップグレード結果のレポートが表示されます。

cppkg

説明

Security Management Server上のSmartUpdateソフトウェアパッケージリポジトリを管理します。

重要 - Gaia OSで動作するSecurity Gatewayでは、SmartUpdateによるソフトウェアパッケージのインストールはサポートされていません。

構文

```
cppkg
      add <options>
      {del | delete} <options>
      get
      getroot
      print
      setroot <options>
```

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、MDSのコンテキストでこのコマンドを実行する必要があります(`mdsenv`を実行)。

パラメータ

パラメータ	説明
`add <options>`	SmartUpdateソフトウェアパッケージをリポジトリに追加します。 参照: *cppkg add (775ページ)*。
`{del | delete} <options>`	リポジトリからSmartUpdateソフトウェアパッケージを削除します。 参照: *ppkg delete (777ページ)*。
`get`	リポジトリのSmartUpdateソフトウェアパッケージのリストを更新します。 参照: *cppkg get (779ページ)*。
`getroot`	リポジトリのルートディレクトリへのパス(環境変数`$SUROOT`の値)を表示します。 参照: *cppkg getroot (780ページ)*。
`print`	リポジトリのSmartUpdateソフトウェアパッケージのリストを表示します。 参照: *cppkg print (781ページ)*。
`setroot <options>`	リポジトリのルートディレクトリへのパスを設定します。 参照: *cppkg setroot (782ページ)*。

cppkg add

説明

SmartUpdateソフトウェアパッケージをSmartUpdateソフトウェアパッケージリポジトリに追加します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、データシートのコンテキストでこのコマンドを実行する必要があります(`mdsenv`コマンドを実行)。
- このコマンドは、既存のパッケージを上書きすることはありません。既存のパッケージを上書きするには、まず既存のパッケージを削除する必要があります。
- SmartUpdateソフトウェアパッケージは、次から入手します: *Check Point Support Center*。

構文

```
cppkg add <Full Path to Package | DVD Drive [Product]>
```

パラメータ

パラメータ	説明
<Full Path to Package>	SmartUpdateソフトウェアパッケージのコンピュータ上のフルローカルパスを指定します。
DVDドライブ `[Product]`	DVDのルートパスを指定します。 例:`/mnt/CPR80`

例 - 1100 Appliance向けR77.20 HFA_75 (R77.20.75) ファームウェアパッケージを追加する場合

```
[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                   Minor Version
-------------------------------------------------------------------------------
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg add /var/log/CP1100_6.0_4_0_-.tgz
Adding package to the repository
Getting the package type...
Extracting the package files...
Copying package to the repository...
Package was successfully added to the repository
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                   Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20Gaia Embedded        R77.20
[Expert@MGMT:0]#
```

ppkg delete

説明

SmartUpdateソフトウェアパッケージをSmartUpdateソフトウェアパッケージリポジトリから削除します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、データシートのコンテキストでこのコマンドを実行する必要があります(`mdsenv`コマンドを実行)。

構文

```
cppkg del ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

```
cppkg delete ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

パラメータ

パラメータ	説明
`del | delete`	オプションのパラメータを指定しない場合、コマンドはインタラクティブモードで実行されます。コマンドは、該当するオプションを含むメニューを表示します。
"<*Vendor*>"	パッケージベンダーを指定します。二重引用符で囲みます。
"<*Product*>"	製品名を指定します。二重引用符で囲みます。
"<*Major Version*>"	パッケージのメジャーバージョンを指定します。二重引用符で囲みます。
"<*OS*>"	パッケージOSを指定します。二重引用符で囲みます。
"<*Minor Version*>"	パッケージのマイナーバージョンを指定します。二重引用符で囲みます。

注：

- オプションパラメータの値を見るには*cppkg print (781ページ)*コマンドを実行します。
- オプションのパラメータをすべて指定するか、パラメータを指定しない必要があります。

例1 - インタラクティブモード

```
[Expert@MGMT:0]# cppkg delete

Select package:
--------------------
(0) Delete all
(1) CP1100 Gaia Embedded Check Point R77.20 R77.20

(e) Exit

Enter your choice : 1

You chose to delete 'CP1100 Gaia Embedded Check Point R77.20 R77.20', Is this correct? [y/n] :
y

Package was successfully removed from the repository
[Expert@MGMT:0]#
```

例2 - 指定したパッケージを手動で削除

```
Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                    Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20Gaia Embedded        R77.20
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg delete "Check Point" "CP1100" "R77.20" "Gaia Embedded" "R77.20"
Package was successfully removed from the repository
[Expert@MGMT:0]#
```

cppkg get

説明

SmartUpdateソフトウェアパッケージのリポジトリにあるSmartUpdateソフトウェアパッケージのリストを、リポジトリの実際の内容に基づいて更新します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、データシートのコンテキストでこのコマンドを実行する必要があります(`mdsenv`コマンドを実行)。

構文

```
cppkg get
```

例

```
[Expert@MGMT:0]# cppkg get
Update successfully completed
[Expert@MGMT:0]#
```

cppkg getroot

説明

SmartUpdateソフトウェアパッケージリポジトリのルートディレクトリへのパス(環境変数`$SUROOT`の値)を表示します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、データシートのコンテキストでこのコマンドを実行する必要があります(`mdsenv`コマンドを実行)。

構文

```
cppkg getroot
```

例

```
[Expert@MGMT:0]# cppkg getroot
[cppkg 7119 4128339728]@MGMT[29 May 19:16:06] Current repository root is set to :
/var/log/cpupgrade/suroot
[Expert@MGMT:0]#
```

cppkg print

説明

SmartUpdateソフトウェアパッケージリポジトリに登録されているSmartUpdateソフトウェアパッケージのリストを表示します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、データシートのコンテキストでこのコマンドを実行する必要があります(`mdsenv`コマンドを実行) 。

構文

```
cppkg print
```

例 - 1100 Appliance向けR77.20 HFA_75 (R77.20.75) ファームウェアパッケージ

```
[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                   Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20Gaia Embedded        R77.20
[Expert@MGMT:0]#
```

cppkg setroot

説明

SmartUpdateソフトウェアパッケージリポジトリのルートディレクトリへのパスを設定します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、データシートのコンテキストでこのコマンドを実行する必要があります(`mdsenv`コマンドを実行)。
- デフォルトのパス: `/var/log/cpupgrade/suroot`
- リポジトリのルートディレクトリを変更する場合:
  - このコマンドは、古いリポジトリから新しいリポジトリにソフトウェアパッケージをコピーします。新しい場所にあるパッケージが古い場所にあるパッケージと同じ名前である場合、そのパッケージは上書きされます。
  - このコマンドは、Check Point Profile シェルスクリプト(`$CPDIR/tmp/.CPprofile.sh`と`$CPDIR/tmp/.CPprofile.csh`)内の環境変数`$SUROOT`の値を更新します。

構文

```
cppkg setroot <Full Path to Repository Root Directory>
```

例

```
[Expert@MGMT:0]# cppkg setroot /var/log/my_directory

Repository root is set to : /var/log/cpupgrade/suroot

Note : When changing repository root directory :

       1. Old repository content will be copied into the new repository
       2. A package in the new location will be overwritten by a package in the old
          location, if the packages have the same name

Change the current repository root ? [y/n] : y

The new repository directory does not exist. Create it ? [y/n] : y

Repository root was set to : /var/log/my_directory

Notice : To complete the setting of your directory, reboot the machine!
[Expert@MGMT:0]#
```

cpprod_util

説明

このユーティリティは、Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) を手動で開くことなく動作させることができます。

- このCheck Pointコンピュータで有効になっているCheck Point製品と機能が表示されます。
- このCheck PointコンピュータのCheck Point製品と機能を有効化および無効化します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

`cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}`
`cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4} "<Value>" {0|1}`
`cpprod_util -dump`

パラメータ

パラメータ	説明
`CPPROD_GetValue`	指定した製品または機能の設定ステータスを取得します。 ■ 0 - 無効 ■ 1 - 有効
`CPPROD_SetValue`	指定した製品または機能のコンフィグレーションを設定します。 **重要** - Check Pointのサポートまたは研究開発部門から明示的な指示がない限り、これらのコマンドを実行しないでください。
"<*Product*>"	製品または機能を指定します。
"<*Parameter*>"	指定された製品または機能の設定パラメータを指定します。
"<*Value*>"	指定された製品または機能の構成パラメータの値を指定します。 ■ 0、1、4のいずれかの整数 ■ 文字列
`dump`	Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) のダンプファイルを現在の作業ディレクトリに作成します。 出力ファイル名は、`RegDump`です。

注

- パラメータを付けずに"cpprod_util"コマンドを実行すると、次のように表示されます。
  - 利用可能なすべての製品および機能のリスト (例: "FwIsFirewallMgmt"、"FwIsLogServer"、"FwIsStandAlone")
  - 製品または機能を構成する際に想定される引数のタイプ ("no-parameter"、"string-parameter"、"integer-parameter")
  - 返された出力のタイプ ("status-output"または"no-output")
- "cpprod_util"コマンドの出力をリダイレクトするには、*stderr*を*stdout*にリダイレクトする必要があります:

```
cpprod_util <options> > <output file> 2>&1
```

例:

```
cpprod_util > /tmp/output_of_cpprod_util.txt 2>&1
```

例

例 - 管理サーバにインストールされているすべてのCheck Point製品パッケージのリストを表示

```
[Expert@MGMT:0]# cpprod_util CPPROD_GetInstalledProducts
CPFC
IDA
MGMT
FW1
SecurePlatform
NGXCMP
EdgeCmp
SFWCMP
SFWR75CMP
SFWR77CMP
FLICMP
R75CMP
R7520CMP
R7540CMP
R76CMP
R77CMP
PROVIDER-1
Reporting Module
SmartLog
CPinfo
VSEC
DIAG
[Expert@MGMT:0]#
```

例 - このCheck Pointのコンピュータが管理サーバとして構成されているかどうかを確認

```
[Expert@MGMT:0]# cpprod_util FwIsFirewallMgmt
1
[Expert@MGMT:0]#
```

例 - このCheck Pointのコンピュータがスタンドアロンとして構成されているかどうかを確認

```
[Expert@MGMT:0]# cpprod_util FwIsStandAlone
0
[Expert@MGMT:0]#
```

例 - この管理サーバがハイアベイラビリティのプライマリとして構成されているかどうかの確認

```
[Expert@MGMT:0]# cpprod_util FwIsPrimary
1
[Expert@MGMT:0]#
```

例 - この管理サーバがハイアベイラビリティでアクティブとして構成されているかどうかを確認

```
[Expert@MGMT:0]# cpprod_util FwIsActiveManagement
1
[Expert@MGMT:0]#
```

例 - この管理サーバがハイアベイラビリティのバックアップとして構成されているかどうかを確認

```
[Expert@MGMT:0]# cpprod_util FwIsSMCBackup
1
[Expert@MGMT:0]#
```

例 - このCheck Pointのコンピュータが専用のログサーバとして構成されているかどうかを確認

```
[Expert@MGMT:0]# cpprod_util FwIsLogServer
1
[Expert@MGMT:0]#
```

例 - この管理サーバでSmartProvisioning Bladeが有効になっているかどうかを確認

```
[Expert@MGMT:0]# cpprod_util FwIsAtlasManagement
1
[Expert@MGMT:0]#
```

例 - この管理サーバでSmartEvent Server Bladeが有効になっているかどうかの確認

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerServer
1
[Expert@MGMT:0]#
```

例 - この管理サーバでSmartEvent Correlation Unit Bladeが有効になっているかどうかを確認

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerCorrelationUnit
1
[Expert@MGMT:0]#
```

例 - この管理サーバでEndpoint Policy Management Bladeが有効になっているかどうかを確認

```
[Expert@MGMT:0]# cpprod_util UepmIsInstalled
1
[Expert@MGMT:0]#
```

例 - この管理サーバがエンドポイントポリシーサーバとして構成されているかどうかの確認

```
[Expert@MGMT:0]# cpprod_util UepmIsPolicyServer
0
[Expert@MGMT:0]#
```

cprid

説明

Check Point Remote Installation Daemon (`cprid`) を管理します。

このデーモンは、管理下のセキュリティゲートウェイに対するCheck Point製品のリモートアップグレードやインストールに使用されます。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、MDSのコンテキストでこれらのコマンドを実行する必要があります(`mdsenv`を実行)。

コマンド

構文	説明
`cpridstart`	Check Point Remote Installation Daemon (`cprid`) を起動します。
`cpridstop`	Check Point Remote Installation Daemon (`cprid`) を停止します。
`run_cprid_restart`	Check Point Remote Installation Daemon (`cprid`) を停止してから起動します。

cprinstall

説明

リモート管理されたセキュリティゲートウェイに対して、Check Point製品パッケージのインストールとそれに伴う作業を実施します。

重要 - このコマンドによるソフトウェアパッケージのインストールは、Gaia OS上で動作するSecurity Gatewayではサポートされていません。

注:

- このコマンドを実行するには、SmartUpdateのライセンスが必要です。
- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

- リモートのSecurity Gatewayでは、以下が必要です。
  - Security Management ServerとSecurity Gateway間でSIC Trustを確立する必要があります。
  - `cpd`デーモンが動作している必要があります。
  - `cprid`デーモンが動作している必要があります。

構文

```
cprinstall
      boot <options>
      cprestart <options>
      cpstart <options>
      cpstop <options>
      delete <options>
      get <options>
      install <options>
      revert <options>
      show <options>
      snapshot <options>
      transfer <options>
      uninstall <options>
      verify <options>
```

パラメータ

パラメータ	説明
`boot <options>`	管理しているSecurity Gatewayを再起動します。 参照: *cprinstall boot (791ページ)*。
`cprestart <options>`	管理するSecurity Gateway上で`cprestart`コマンドを実行します。 参照: *cprinstall cprestart (792ページ)*。
`cpstart <options>`	管理するSecurity Gateway上で`cpstart`コマンドを実行します。 参照: *cprinstall cpstart (793ページ)*。
`cpstop <options>`	管理するSecurity Gateway上で`cpstop`コマンドを実行します。 参照: *cprinstall cpstop (794ページ)*。
`delete <options>`	管理対象のSecurity Gatewayのスナップショット(バックアップ)ファイルを削除します。 参照: *cprinstall delete (795ページ)*。
`get <options>`	■ 管理対象のSecurity Gatewayにインストールされている製品およびOSの詳細を取得します。 ■ Security Management Server上の管理データベースを更新します。 参照: *cprinstall get (796ページ)*。
`install <options>`	管理下のSecurity GatewayにCheck Point製品をインストールします。 参照: *cprinstall install (797ページ)*。
`revert <options>`	SecurePlatform OS上で動作するマネージドセキュリティゲートウェイを、そのセキュリティゲートウェイに保存されたスナップショットから復元します。 参照: *cprinstall revert (800ページ)*。
`show <options>`	SecurePlatform OS上で動作する管理対象Security Gatewayのすべてのスナップショット(バックアップ)ファイルを表示します。 参照: *cprinstall show (801ページ)*。
`snapshot <options>`	SecurePlatform OS上で動作する管理対象Security Gatewayにスナップショットを作成し、そのSecurity Gatewayに保存します。 参照: *cprinstall snapshot (802ページ)*。
`transfer <options>`	パッケージをインストールせずに、リポジトリから管理対象Security Gatewayにソフトウェアパッケージを転送します。 参照: *cprinstall transfer (803ページ)*。
`uninstall <options>`	管理対象Security GatewayのCheck Point製品をアンインストールします。 参照: *cprinstall uninstall (804ページ)*。

パラメータ	説明
`verify <options>`	次の操作が成功したことを確認します。 ■ 管理対象のSecurity Gatewayに特定の製品をインストールできる場合。 ■ 管理対象のセキュリティゲートウェイのオペレーティングシステム及び現在インストールされている製品が、ソフトウェアパッケージに適切であること。 ■ 管理対象のSecurity Gatewayをインストールするのに十分なディスク容量があること。 ■ 管理対象のセキュリティゲートウェイとCPRID接続があること。 参照: *cprinstall verify (806ページ)*。

cprinstall boot

説明

管理しているSecurity Gatewayを再起動します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cprinstall boot <Object Name>
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。

例

```
[Expert@MGMT]# cprinstall boot MyGW
```

cprinstall cprestart

説明

管理するSecurity Gateway上でcprestartコマンドを実行します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

- 管理対象のSecurity Gatewayに搭載されている Check Point製品は、すべて同じバージョンである必要があります。

構文

```
cprinstall cprestart <Object Name>
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。

例

```
[Expert@MGMT:0]# cprinstall cprestart MyGW
```

cprinstall cpstart

説明

管理するSecurity Gateway上でcpstartコマンドを実行します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

- 管理対象のSecurity Gatewayに搭載されている Check Point製品は、すべて同じバージョンである必要があります。

構文

```
cprinstall cpstart <Object Name>
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。

例

```
[Expert@MGMT]# cprinstall cpstart MyGW
```

cprinstall cpstop

説明

管理するSecurity Gateway上でcpstopコマンドを実行します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

- 管理対象のSecurity Gatewayに搭載されている Check Point製品は、すべて同じバージョンである必要があります。

構文

```
cprinstall cpstop {-proc | -nopolicy} <Object Name>
```

パラメータ

パラメータ	説明
-proc	Check Pointのデーモンとセキュリティサーバを強制終了しますが、Check Pointのカーネルで実行されているアクティブなセキュリティポリシーは維持されます。サービスに基づく一般的な*許可*、*ドロップ*、*拒否*アクションを持つルールは、引き続き機能します。
-nopolicy	Check PointデーモンとSecurity Serverを停止し、Check Pointカーネルから Security Policyをアンロードします。
<*Object Name*>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。

例

```
[Expert@MGMT]# cprinstall cpstop -proc MyGW
```

cprinstall delete

説明

SecurePlatform OS上で動作するマネージドセキュリティゲートウェイ上のスナップショット(バックアップ)ファイルを削除します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cprinstall delete <Object Name> <Snapshot File>
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。
<Snapshot File>	SecurePlatform OS上のスナップショット(バックアップ)の名前を指定します。

例

```
[Expert@MGMT]# cprinstall delete MyGW Snapshot25Apr2017
```

cprinstall get

説明

- 管理対象のSecurity Gatewayにインストールされている製品およびOSの詳細を取得します。
- Security Management Server上の管理データベースを更新します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cprinstall get <Object Name>
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。

例:

```
[Expert@MGMT]# cprinstall get MyGW
Checking cprid connection...
Verified
Operation completed successfully
Updating machine information...
Update successfully completed
'Get Gateway Data' completed successfully
Operating system   Major Version      Minor Version
-------------------------------------------------------------------------
SecurePlatform     R75.20R75.20

Vendor             Product            Major Version       Minor Version
-------------------------------------------------------------------------
Check Point        VPN-1 Power/UTM    R75.20R75.20Check Point        SecurePlatform
R75.20R75.20Check Point        SmartPortal        R75.20R75.20
[Expert@MGMT]#
```

cprinstall install

説明

管理下のSecurity GatewayにCheck Point製品をインストールします。

重要 - このコマンドによるソフトウェアパッケージのインストールは、Gaia OSを実行するセキュリティゲートウェイではサポートされていません。

注:

- ソフトウェアパッケージを転送する前に、このコマンドは次を実行します: *cprinstall verify (806ページ)*コマンドを実行します。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- パッケージ属性の値を見るには*cppkg print (781ページ)*コマンドを実行します。

構文

```
cprinstall install [-boot] [-backup] [-skip_transfer] <Object
Name> "<Vendor>" "<Product>" "<Major Version>" "<Minor Version>"
```

パラメータ

パラメータ	説明
`-boot`	パッケージのインストール後、管理されたSecurity Gatewayを再起動します。 **注** - すべての製品が同じバージョンになってから再起動してください。特定のシナリオでは再起動がキャンセルされます。
`-backup`	パッケージをインストールする前に、管理されたSecurity Gateway上にスナップショットを作成します。 **注** - SecurePlatform OS で動作するSecurity Gatewayのみ。
`-skip_transfer`	パッケージの転送をスキップします。
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。
"*<Vendor>*"	パッケージベンダーを指定します。二重引用符で囲みます。 例: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	製品名を指定します。二重引用符で囲みます。 例: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100` ■ `VPN-1 Power/UTM` ■ `SmartPortal`
"*<Major Version>*"	パッケージのメジャーバージョンを指定します。二重引用符で囲みます。
"*<Minor Version>*"	パッケージのマイナーバージョンを指定します。二重引用符で囲みます。

例

```
[Expert@MGMT]# cprinstall install -boot MyGW "checkpoint" "firewall" "R75" "R75.20"

Installing firewall R75.20 on MyGW...
Info : Testing Check Point Gateway
Info : Test completed successfully.
Info : Transferring Package to Check Point Gateway
Info : Extracting package on Check Point Gateway
Info : Installing package on Check Point Gateway
Info : Product was successfully applied.
Info : Rebooting the Check Point Gateway
Info : Checking boot status
Info : Reboot completed successfully.
Info : Checking Check Point Gateway
Info : Operation completed successfully.
[Expert@MGMT]#
```

cprinstall revert

説明

SecurePlatform OS上で動作するマネージドセキュリティゲートウェイを、そのセキュリティゲートウェイに保存されたスナップショットから復元します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cprinstall revert <Object Name> <Snapshot File>
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。
<Snapshot File>	SecurePlatformのスナップショットファイルの名前。 保存されたスナップショットファイルの名前を確認するには*cprinstall show (801ページ)*コマンドを実行します。

cprinstall show

説明

SecurePlatform OS上で動作する管理対象Security Gatewayのすべてのスナップショット(バックアップ)ファイルを表示します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cprinstall show <Object Name>
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。

例

```
[Expert@MGMT]# cprinstall show GW1
SU_backup.tzg
[Expert@MGMT]#
```

cprinstall snapshot

説明

SecurePlatform OS上で動作する管理対象Security Gatewayにスナップショットを作成し、そのSecurity Gatewayに保存します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
cprinstall snapshot <Object Name> <Snapshot File>
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。
<Snapshot File>	SecurePlatformのスナップショットファイルの名前。 保存されたスナップショットファイルの名前を確認するには*cprinstall show (801ページ)*コマンドを実行します。

cprinstall transfer

説明

パッケージをインストールせずに、リポジトリから管理対象Security Gatewayにソフトウェアパッケージを転送します。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

- パッケージ属性の値を見るには*cppkg print (781ページ)*コマンドを実行します。

構文

```
cprinstall transfer <Object Name> "<Vendor>" "<Product>" "<Major Version>" "<Minor Version>"
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。
"*<Vendor>*"	パッケージベンダーを指定します。二重引用符で囲みます。 例: ■ checkpoint ■ Check Point
"*<Product>*"	製品名を指定します。二重引用符で囲みます。 例: ■ SVNfoundation ■ firewall ■ floodgate ■ CP1100
"*<Major Version>*"	パッケージのメジャーバージョンを指定します。二重引用符で囲みます。
"*<Minor Version>*"	パッケージのマイナーバージョンを指定します。二重引用符で囲みます。

cprinstall uninstall

説明

管理対象Security GatewayのCheck Point製品をアンインストールします。

重要 - このコマンドによるソフトウェアパッケージのアンインストールは、Gaia OS上で動作するSecurity Gatewayではサポートされていません。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

- 製品パッケージをアンインストールする前に、このコマンドは次を実行します: *cprinstall verify (806ページ)*コマンドを実行します。
- 製品パッケージをアンインストールした後は、次を実行: *cprinstall get (796ページ)*コマンドを実行します。
- パッケージ属性の値を見るには*cppkg print (781ページ)*コマンドを実行します。

構文

```
cprinstall uninstall [-boot] <Object Name> "<Vendor>" "<Product>"
"<Major Version>" "<Minor Version>"
```

パラメータ

パラメータ	説明
-boot	パッケージのアンインストール後、管理対象Security Gatewayを再起動します。 **注** - 再起動は特定のシナリオでキャンセルされます。
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。
"*<Vendor>*"	パッケージベンダーを指定します。二重引用符で囲みます。 例: ■ checkpoint ■ Check Point
"*<Product>*"	製品名を指定します。二重引用符で囲みます。 例: ■ SVNfoundation ■ firewall ■ floodgate ■ CP1100
"*<Major Version>*"	パッケージのメジャーバージョンを指定します。二重引用符で囲みます。
"*<Minor Version>*"	パッケージのマイナーバージョンを指定します。二重引用符で囲みます。

例

```
[Expert@MGMT]# cprinstall uninstall MyGW "checkpoint" "firewall" "R75.20" "R75.20"
Uninstalling firewall R75.20 from MyGW...
Info : Removing package from Check Point Gateway
Info : Product was successfully applied.
Operation Success. Please get network object data to complete the operation.
[Expert@MGMT]#
[Expert@MGMT]# cprinstall get
```

cprinstall verify

説明

次の操作が成功したことを確認します。

- 管理対象のSecurity Gatewayに特定の製品をインストールできる場合。
- 管理対象のセキュリティゲートウェイのオペレーティングシステム及び現在インストールされている製品が、ソフトウェアパッケージに適切であること。
- 管理対象のSecurity Gatewayをインストールするのに十分なディスク容量があること。
- 管理対象のセキュリティゲートウェイとCPRID接続があること。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

- パッケージ属性の値を見るには*cppkg print (781ページ)*コマンドを実行します。

構文

```
cprinstall verify <Object Name> "<Vendor>" "<Product>" "<Major
Version>" ["<Minor Version>"]
```

パラメータ

パラメータ	説明
<Object Name>	SmartConsoleで設定されたSecurity Gatewayオブジェクトの名前。
"*<Vendor>*"	パッケージベンダーを指定します。二重引用符で囲みます。 例: ■ checkpoint ■ Check Point
"*<Product>*"	製品名を指定します。二重引用符で囲みます。 例: ■ SVNfoundation ■ firewall ■ floodgate ■ CP1100 ■ VPN-1 Power/UTM ■ SmartPortal
"*<Major Version>*"	パッケージのメジャーバージョンを指定します。二重引用符で囲みます。
"*<Minor Version>*"	パッケージのマイナーバージョンを指定します。二重引用符で囲みます。 このパラメータはオプションです。

例1 - 検証に成功

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway.
Info : Test completed successfully.
Info : Installation Verified, The product can be installed.
```

例2 - 検証に失敗した場合

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway
Info : SVN Foundation R75 is already installed on 192.0.2.134
Operation Success. Product cannot be installed, did not pass dependency check.
```

cpstart

説明

すべてのCheck Pointプロセスおよびアプリケーションを手動で起動します。

注:

- `cprid`デーモンには次を使用: *cprid (787ページ)*コマンドを実行します。
- 特定のCheck Pointプロセスを手動で起動する方法については、sk97638を参照してください。

構文

```
cpstart
```

cpstat

説明

Check Pointアプリケーションのステータスおよび統計情報を表示します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

注 - 構文の中のパラメータは、どのような順番で書いてもかまいません。

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 該当するSNMP OIDに対するSNMPクエリとSNMPレスポンスが出力されます。
`-h <Host>`	オプションです。 Management Serverでこのコマンドを実行する場合、このパラメータは管理対象のSecurity Gateway / ClusterXLオブジェクトを指定します。 *<Host>*はIPv4アドレス、解決可能なホスト名、またはDAIPオブジェクト名です。 デフォルトは`localhost`です。
`-p <Port>`	オプションです。 アプリケーションモニタリング(AMON) サーバのポート番号。 デフォルトのポートは18192です。
`-s <SICname>`	オプションです。 アプリケーションモニタリング(AMON) サーバのSIC(Secure Internal Communication) 名。

パラメータ	説明
`-f <Flavor>`	オプションです。 収集する情報の種類を指定します。 フレーバーを明示的に指定しない場合、コマンドは`<Application Flag>`にある最初のフレーバーを使用します。すべてのフレーバーを表示するには、パラメータを指定せずに`cpstat`コマンドを実行します。
`-o <Polling Interval>`	オプションです。 ポーリング間隔(秒)を指定します(コマンドが情報を収集して表示する頻度)。 例: ■ 0 - コマンドは結果を一度だけ表示し、停止します(デフォルト値)。 ■ 5 - コマンドは、5秒ごとにループで結果を表示します。 ■ 30 - コマンドは、30秒ごとにループで結果を表示します。 ■ N - コマンドは、ループの中でN秒ごとに結果を表示します。 このパラメータは、"`-c <Count>`"パラメータと"`-e <Period>`"パラメータと一緒に使用します。 例: `cpstat os -f perf -o 2`
`-c <Count>`	オプションです。 コマンドが停止するまでに何回実行し、結果を表示するかを指定します。 このパラメータは、"`-o <Polling Interval>`"パラメータと一緒に使用する必要があります。 例: ■ 0 - コマンドは、`<Polling Interval>`毎に繰り返し結果を表示します(これがデフォルト値)。 ■ 10 - コマンドは、`<Polling Interval>`毎に10回結果を表示し、その後停止します。 ■ 20 - コマンドは、`<Polling Interval>`毎に20回結果を表示し、その後停止します。 ■ N - コマンドは、`<Polling Interval>`毎にN回結果を表示し、その後停止します。 例: `cpstat os -f perf -o 2 -c 2`

パラメータ	説明
`-e <Period>`	オプションです。 統計情報を計算する時間(秒)を指定します。 このパラメータは、"`-o <Polling Interval>`"パラメータと一緒に使用する必要があります。 このパラメータは、"`-c <Count>`"パラメータと一緒に使用することができます。 例: `cpstat os -f perf -o 2 -c 2 -e 60`
`<Application Flag>`	必須です。 アプリケーションフラグのフレーバーは下表を参照してください。

これらのフレーバーはアプリケーションフラグで利用可能です。

注 - 使用可能なフラグは、有効なSoftware Bladeによって異なります。Security Gateway / ClusterXLでのみサポートされるフラグと、Management Serverでのみサポートされるフラグがあります。

機能またはSoftware Blade	フラグ	フレーバー
有効なSoftware Bladeのリスト	`blades`	`fw, ips, av, urlf, vpn, cvpn, aspm, dlp, appi, anti_bot, default, content_awareness, threat-emulation, default`
オペレーティングシステム	`os`	`default, ifconfig, routing, routing6, memory, old_memory, cpu, disk, perf, multi_cpu, multi_disk, raidInfo, sensors, power_supply, hw_info, all, average_cpu, average_memory, statistics, updates, licensing, connectivity, vsx`
ファイアウォール	`fw`	`default, interfaces, policy, perf, hmem, kmem, inspect, cookies, chains, fragments, totals, totals64, ufp, http, ftp, telnet, rlogin, smtp, pop3, sync, log_connection, all`
HTTPSインスペクション	`https_inspection`	`default, hsm_status, all`

機能または Software Blade	フラグ	フレーバー
アイデンティティアウェアネス	identityServer	default, authentication, logins, ldap, components, adquery, idc, muh
アプリケーションコントロール	appi	default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month
URL フィルタリング	urlf	default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month
IPS	ips	default, statistics, all
アンチウイルス	ci	default
脅威対策	antimalware	default, scanned_hosts, scanned_mails, subscription_status, update_status, ab_prm_contracts, av_prm_contracts, ab_prm_contracts, av_prm_contracts
Threat Emulation	threat-emulation	default, general_statuses, update_status, scanned_files, malware_detected, scanned_on_cloud, malware_on_cloud, average_process_time, emulated_file_size, queue_size, peak_size, file_type_stat_file_scanned, file_type_stat_malware_detected, file_type_stat_cloud_scanned, file_type_stat_cloud_malware_scanned, file_type_stat_filter_by_analysis, file_type_stat_cache_hit_rate, file_type_stat_error_count, file_type_stat_no_resource_count, contract, downloads_information_current, downloading_file_information, queue_table, history_te_incidents, history_te_comp_hosts

機能または Software Blade	フラグ	フレーバー
Threat Extraction	scrub	default, subscription_status, threat_extraction_statistics
モバイルアクセス	cvpn	cvpnd, sysinfo, products, overall
VSX	vsx	default, stat, traffic, conns, cpu, all, memory, cpu_usage_per_core
IPsec VPN	vpn	default, product, IKE, ipsec, traffic, compression, accelerator, nic, statistics, watermarks, all
DLP (データ損失防止)	dlp	default, dlp, exchange_agents, fingerprint
コンテンツアウェアネス	ctnt	default
QoS	fg	all
ハイ・アベイラビリティ	ha	default, all
リモートアクセス VPNクライアント用ポリシーサーバ	polsrv	default, all
リモートアクセス VPNクライアント用デスクトップポリシーサーバ	dtps	default, all
LTE / GX	gx	default, contxt_create_info, contxt_delete_info, contxt_update_info, contxt_path_mng_info, GXSA_GPDU_info, contxt_initiate_info, gtpv2_create_info, gtpv2_delete_info, gtpv2_update_info, gtpv2_path_mng_info, gtpv2_cmd_info, all
管理サーバ	mg	default, log_server, indexer
証明書認証局	ca	default, crl, cert, user, all

機能または Software Blade	フラグ	フレーバー
SmartEvent	`cpsemd`	`default`
SmartEvent相関ユニット	`cpsead`	`default`
ログサーバ	`ls`	`default`
CloudGuard Controller	`vsec`	`default`
SmartReporter	`svr`	`default`
Provisioning Agent	`PA`	`default`
"`threshold_config`"コマンドで設定されたしきい値	`thresholds`	`default, active_thresholds, destinations, error`
過去のステータス値	`persistency`	`product, TableConfig, SourceConfig`

例

例 - CPU使用率

```
[Expert@HostName:0]# cpstat -f cpu os
CPU User Time (%):   1
CPU System Time (%): 0
CPU Idle Time (%):   99
CPU Usage (%):       1
CPU Queue Length:    -
CPU Interrupts/Sec:  172
CPUs Number:         8

[Expert@HostName:0]#
```

例 - パフォーマンス

```
[Expert@HostName:0]# cpstat os -f perf -o 2 -c 2 -e 60

Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741331456
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741331456
Free Real Memory (Bytes):                4489732096
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       0
CPU System Time (%):                     0
CPU Idle Time (%):                       100
CPU Usage (%):                           0
CPU Queue Length:                        -
CPU Interrupts/Sec:                      135
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296


Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741556736
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741556736
Free Real Memory (Bytes):                4489506816
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       3
CPU System Time (%):                     0
CPU Idle Time (%):                       97
CPU Usage (%):                           3
CPU Queue Length:                        -
CPU Interrupts/Sec:                      140
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296

[Expert@HostName:0]#
```

例 - 管理サーバの現在の接続セッションのリスト

```
[Expert@MGMT:0]# cpstat -f default mg

Product Name:  Check Point Security Management Server
Major version: 6
Minor version: 0
Build number:  994000031
Is started:    1
Active status: active
Status:        OK

Connected clients
-----------------------------------------------------
|Client type |Administrator|Host        |Database lock|
-----------------------------------------------------
|SmartConsole|admin        |JOHNDOE-PC  |false        |
-----------------------------------------------------

[Expert@MGMT:0]#
```

cpstop

説明

すべてのCheck Pointのプロセスおよびアプリケーションを手動で停止します。

注:

- `cprid`デーモンには次を使用: *cprid (787ページ)*コマンドを実行します。
- 特定のCheck Pointプロセスを手動で停止する方法については、sk97638を参照してください。

構文

```
cpstop
```

cpview

CPViewの概要

説明

CPViewは、Check Pointコンピュータに内蔵されているテキストベースのユーティリティです。

CPViewユーティリティは、一般的なシステム情報(CPU、メモリ、ディスクスペース)と、異なるSoftware Bladeの情報(Security Gateway / ClusterXL / Scalable Platform Security Groupのみ)の両方を含む統計データを表示します。

CPViewは、アクセスしやすいビューでデータを継続的に更新します。

Security Gateway / ClusterXL / Scalable Platform Security Groupでは、この統計データを使用してパフォーマンスを監視することができます。

詳細は、sk101878を参照してください。

構文

```
cpview --help
```

CPViewユーザインタフェース

CPViewのユーザインタフェースは、3つのセクションから構成されています。

セクション	説明
Header	このビューには、3番目のビューの統計が収集された時間が表示されます。 統計情報を更新したときに更新されます。
Navigation	このメニューバーは、インタラクティブなものです。メニュー間の移動は、矢印キーとマウスを使用します。 メニューにはサブメニューがあり、メニューバーの下に表示されます。
View	このビューには、そのビューで収集された統計情報が表示されます。 これらの統計情報は、リフレッシュレートで更新されます。

CPViewの使用

CPViewの操作には次のキーを使用します。

キー	説明
矢印キー	メニューとビューの間を移動します。ビューをスクロールします。
Home	Overviewのビューに戻ります。
Enter	View Modeに変わります。 サブメニューのあるメニューでは、Enterキーで最下層のサブメニューに移動します。
Esc	Menu Modeに戻ります。
Q	CPViewを終了します。

これらのキーを使用して、CPViewのインタフェースオプションを変更します。

キー	説明
R	リフレッシュレートを変更するウィンドウが開きます。 デフォルトのリフレッシュレートは2秒です。
W	ワイド表示と通常表示の切り替えを行います。 ワイドモードでは、CPViewは画面を水平方向に合わせます。
S	行数またはカラム数を手動で設定します。
M	マウスのオン/オフを切り替えます。
P	統計情報の収集を一時停止および再開します。

これらのキーは、統計情報の保存、ヘルプの表示、統計情報の更新に使用します。

キー	説明
C	現在のページをファイルに保存します。ファイル名の形式は次のとおりです。 `cpview_<ID of the cpview process>.cap<Number of the capture>`
H	CPViewのオプションをツールチップで表示します。
スペースバー	統計をただちに更新します。

cpwd_admin

説明

Check Point WatchDog (cpwd) は、ローカルコンピュータ上のCheck Pointデーモンなどの重要なプロセスを呼び出してモニタし、そのプロセスに障害が発生した場合に再起動を試みるプロセスです。

Watchdogがモニタするプロセスにはfwm,fwd、cpd、DAServiceなどがあります。

モニタされるプロセスのリストは、インストールおよび設定されているCheck Point製品およびSoftware Bladeによって異なります。

Check Point WatchDogは、モニタ情報を$CPDIR/log/cpwd.elgのログファイルに書き込みます。

cpwd_adminユーティリティは、モニタするプロセスの状態を表示し、Check Point WatchDogの設定を行います。

Check Point WatchDogのモニタリングには2つのタイプがあります。

モニタリング	説明
パッシブ	WatchDogは、プロセスが異常終了した場合にのみ、プロセスを再起動する。 cpwd_admin listコマンドの出力では、MONカラムにパッシブにモニタされるプロセスのNが表示されます。
アクティブ	WatchDogは、事前定義された間隔ごとにプロセスの状態をチェックします。 WatchDogは、プロセスが生きていること、また正しく機能していること(デッドロックに陥っていない、フリーズしていないなど) を確認します。 cpwd_admin listコマンドの出力では、MONカラムにアクティブにモニタされているプロセスのYが表示されます。 アクティブにモニタされるプロセスの一覧は、Check Pointによって事前に定義されています。ユーザが変更したり設定したりすることはできません。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

パラメータ

パラメータ	説明
`config <options>`	Check Point WatchDogを設定します。 参照: *cpwd_admin config (822ページ)*。
`del <options>`	監視対象プロセスを監視対象プロセスのWatchDogデータベースから一時的に削除します。 参照: *cpwd_admin del (825ページ)*。
`detach <options>`	モニタしているプロセスをWatchDogのモニタから一時的に切り離します。 参照: *cpwd_admin detach (826ページ)*。
`exist`	WatchDogプロセス`cpwd`が生きているかどうかチェックします。 参照: *cpwd_admin exist (827ページ)*。
`flist <options>`	すべてのモニタしているプロセスの状態を`$CPDIR/tmp/cpwd_list_<Epoch Timestamp>.lst`ファイルに保存します。 参照: *cpwd_admin flist (828ページ)*。
`getpid <options>`	モニタしているプロセスのPIDを表示します。 参照: *cpwd_admin getpid (830ページ)*。

パラメータ	説明
`kill <options>`	WatchDogプロセス`cpwd`を終了します。 参照: *cpwd_admin kill (831ページ)*。 **重要** - Check Pointのサポートまたは R&Dから明示的に指示がない限り、このコマンドを実行**しないで**ください。
`list`	モニタしているすべてのプロセスの状態を画面に表示します。 参照: *cpwd_admin list (832ページ)*。
`monitor_list`	アクティブモニタリング対象プロセスの状態を画面に表示します。 参照: *cpwd_admin monitor_list (835ページ)*。
`start <options>`	WatchDogがモニタしているプロセスを開始します。 参照: *cpwd_admin start (836ページ)*。
`start_monitor`	WatchDogのアクティブモニタリングを開始 - 事前に定義されたプロセスをWatchDogでアクティブにモニタリングします。 参照: *cpwd_admin start_monitor (838ページ)*。
`stop <options>`	モニタしているプロセスを停止します。 参照: *cpwd_admin stop (839ページ)*。
`stop_monitor`	WatchDogのアクティブなモニタリングを停止 - 全てのプロセスをパッシブにのみモニタします。 参照: *cpwd_admin stop_monitor (841ページ)*。

cpwd_admin config

説明

Check Point WatchDogを設定します。

重要 - WatchDog 構成パラメータを変更した後は、「`cpstop`」および「`cpstart`」コマンド(すべてのCheck Pointプロセスを再起動する) を使用して WatchDog プロセスを再起動する必要があります。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

パラメータ

パラメータ	説明
`-h`	ビルトインの使用状況を表示します。
`-a <Configuration_Parameter_1>=<Value_1> <Configuration_Parameter_2>=<Value_2> ... <Configuration_Parameter_N>=<Value_N>`	WatchDogの設定パラメータを追加します。 **注** - 設定パラメータ名、等号、値の間にスペースを入れてはいけません。
`-d <Configuration_Parameter_1> <Configuration_Parameter_2> ... <Configuration_Parameter_N>`	`cpwd_admin config -a`"コマンドでユーザが追加したWatchDogの設定パラメータを削除します。
`-p`	ユーザが"`cpwd_admin config -a`"コマンドで追加したWatchDog設定パラメータを表示します。
`-r`	WatchDogのデフォルト設定を復元します。

利用可能な設定パラメータと可能な値:

設定パラメータ	可能な値	説明
no_limit	■ 範囲 : -1、0、>0 ■ デフォルト : 5	rerun_mode=1の場合、WatchDogがプロセスの再起動を試みる最大回数を指定。 ■ -1 - 常に再起動を試みます ■ 0 - 再起動を試みない ■ >0 - この回数を試す
num_of_procs	■ 範囲 : 30 - 20000 ■ デフォルト : 10000	WatchDogが管理するプロセスの最大数を設定。
rerun_mode	■ 0 ■ 1 (デフォルト)	WatchDogが失敗した後にプロセスを再起動させるかどうかを設定します。 ■ 0 - 失敗したプロセスを再起動しません。モニタとログ記録の行います。 ■ 1 - 失敗したプロセスを再起動します (これがデフォルト)。
reset_startups	■ 範囲 : > 0 ■ デフォルト : 3600	プロセスの開始後、WatchDogがプロセスのstartup_counterを0にリセットするまでのWatchDogの待機時間 (秒) を設定します。 プロセスの起動カウンタを確認するには、cpwd_admin listコマンドの出力で#STARTのカラムを参照します。
sleep_mode	■ 0 ■ 1 (デフォルト)	WatchDogがプロセスを再起動する方法を設定します。 ■ 0 - タイムアウトを無視して直ちに処理を再開する ■ 1 - この時間待機sleep_timeout
sleep_timeout	■ 範囲 : 0 - 3600 ■ デフォルト : 60	rerun_mode=1の場合、プロセスの失敗からWatchDogが再起動を試みるまでの時間 (秒単位) を指定します。
stop_timeout	■ 範囲 : > 0 ■ デフォルト : 60	プロセス停止コマンドが完了するまでのWatchDogの待機時間 (秒) を設定します。
zero_timeout	■ 範囲 : > 0 ■ デフォルト : 7200	プロセスの再起動にno_limit回失敗した後、WatchDogは再試行する前にzero_timeout秒間待機します。 zero_timeoutの値はtimeoutの値より大きくなければなりません。

WatchDogはユーザ定義の設定パラメータを$CPDIR/registry/HKLM_registry.dataファイルの": (Wd_Config" セクションに保存します。

```
("CheckPoint Repository Set"
  : (SOFTWARE
    : (CheckPoint
      : (CPshared
        :CurrentVersion (6.0)
        : (6.0
        ... ...
          : (reserved
          ... ...
            : (Wd
                : (Wd_Config
                    :Configuration_Parameter_1 ("[4]Value_1"):Configuration_Parameter_2 ("
[4]Value_2")
                )
            )
          ... ...
```

例

```
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -a sleep_timeout=120 no_limit=12
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog Configuration parameters are:
sleep_timeout : 120
no_limit : 12
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#

[Expert@HostName:0]# cpwd_admin config -r
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
```

cpwd_admin del

説明

監視対象プロセスを監視対象プロセスのWatchDogデータベースから一時的に削除します。

注:

- WatchDogは切り離されたプロセスのモニタを停止しますが、プロセス自体は維持されます。
- 割り当てられたロールの*cpwd_admin list (832ページ)*コマンドは、削除されたプロセスは表示されません。
- この変更は、ブート中にすべてのCheck Pointサービスが再起動するまで適用されます。*cpstart (808ページ)*コマンドを実行します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin del -name <Application Name>
```

パラメータ

パラメータ	説明
<Application Name>	出力に表示されるCheck Pointのモニタ対象プロセス名 *cpwd_admin list (832ページ)*コマンド(左端のカラムAPP)。 例: ■ FWM ■ FWD ■ CPD ■ CPM

例

```
[Expert@HostName:0]# cpwd_admin del -name FWD
cpwd_admin:
successful Del operation
[Expert@HostName:0]#
```

cpwd_admin detach

説明

モニタしているプロセスをWatchDogのモニタから一時的に切り離します。

注:

- WatchDogは切り離されたプロセスのモニタを停止しますが、プロセス自体は維持されます。
- 割り当てられたロールの*cpwd_admin list (832ページ)*コマンドは、デタッチされたプロセスは表示されません。
- この変更は、ブート中にすべてのCheck Pointサービスが再起動するまで適用されます。*cpstart (808ページ)*コマンドを実行します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin detach -name <Application Name>
```

パラメータ

パラメータ	説明
<Application Name>	出力に表示されるCheck Pointのモニタ対象プロセス名。*cpwd_admin list (832ページ)*コマンド(左端のカラムAPP)。 例: ■ FWM ■ FWD ■ CPD ■ CPM

例

```
[Expert@HostName:0]# cpwd_admin detach -name FWD
cpwd_admin:
successful Detach operation
[Expert@HostName:0]#
```

cpwd_admin exist

説明

WatchDogプロセスcpwdが生きているかどうかチェックします。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin exist
```

例

```
[Expert@HostName:0]# cpwd_admin exist
 cpwd_admin: cpWatchDog is running
[Expert@HostName:0]#
```

cpwd_admin flist

説明

WatchDogがモニタしている全てのプロセスの状態をファイルに保存します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin flist [-full]
```

パラメータ

パラメータ	説明
-full	詳細出力を表示します。

出力

カラム	説明
APP	モニタしているプロセスのWatchDog名を表示します。
PID	モニタしているプロセスのPIDを表示します。
STAT	モニタしているプロセスの状態を表示します。 ■ E- 実行 ■ T- 終了
#START	WatchDogがモニタプロセスを何回開始したかを示します。
START_TIME	WatchDogがモニタプロセスを最後に開始した時刻を表示します。
SLP/LIMIT	冗長出力では、sleep_timeoutとno_limit設定パラメータの値を表示 (*cpwd_admin config (822ページ)*)。
MON	WatchDogでのこのプロセスの監視方法を表示 (*cpwd_admin (819ページ)*): ■ Y- アクティブモニタリング ■ N- パッシブモニタリング
COMMAND	WatchDogがこのプロセスを開始するために実行したコマンドが表示されます。

例

```
[Expert@HostName:0]# cpwd_admin flist
/opt/CPshrd-R82/tmp/cpwd_list_1564617600.lst
[Expert@HostName:0]#
```

cpwd_admin getpid

説明

WatchDogがモニタしているプロセスのPIDを表示します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin getpid -name <Application Name>
```

パラメータ

パラメータ	説明
<Application Name>	出力に表示されるCheck Pointのモニタ対象プロセス名。*cpwd_admin list (832ページ)*コマンド(左端のカラムAPP)。 例: ■ FWM ■ FWD ■ CPD ■ CPM

例

```
[Expert@HostName:0]# cpwd_admin getpid -name FWD
5640
[Expert@HostName:0]#
```

cpwd_admin kill

説明

WatchDogプロセス`cpwd`を終了します。

重要 - Check Pointのサポートまたは R&Dから明示的に指示がない限り、このコマンドを実行**しないで**ください。
WatchDogプロセスの再起動には、すべてのCheck Pointサービスを再起動する*cpstop (816ページ)*と*cpstart (808ページ)*コマンドを使用します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin kill
```

cpwd_admin list

説明

WatchDogがモニタしている全てのプロセスの状態を画面に表示します。

注 - デフォルトでは、WatchDogは最大10000プロセスをモニタします。
この閾値を上げるには、"`cpwd_admin config -a num_of_procs=<value>`"コマンドを使います。
参照: *cpwd_admin config (822ページ)*。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin list [-full]
```

パラメータ

パラメータ	説明
`-full`	詳細出力を表示します。

出力

カラム	説明
APP	モニタしているプロセスのWatchDog名を表示します。
PID	モニタしているプロセスのPIDを表示します。
STAT	モニタしているプロセスの状態を表示します。 ■ E- 実行 ■ T- 終了
#START	WatchDogがモニタプロセスを何回開始したかを示します。
START_TIME	WatchDogがモニタプロセスを最後に開始した時刻を表示します。
SLP/LIMIT	冗長出力では、sleep_timeoutとno_limit設定パラメータの値を表示 (*cpwd_admin config (822ページ)*)。
MON	WatchDogでのこのプロセスの監視方法を表示(*cpwd_admin (819ページ)*): ■ Y- アクティブモニタリング ■ N- パッシブモニタリング
COMMAND	WatchDogがこのプロセスを開始するために実行したコマンドが表示されます。

例

例 - 管理サーバのデフォルト出力

```
[Expert@HostName:0]# cpwd_admin list
APP         PID    STAT  #START  START_TIME             MON  COMMAND
CPVIEWD     19738  E     1       [17:50:44] 31/5/2019   N    cpviewd
HISTORYD    0      T     0       [17:54:44] 31/5/2019   N    cpview_historyd
CPD         19730  E     1       [17:54:45] 31/5/2019   Y    cpd
SOLR        19935  E     1       [17:50:55] 31/5/2019   N    java_solr /opt/CPrt-
R82/conf/jetty.xml
RFL         19951  E     1       [17:50:55] 31/5/2019   N    LogCore
SMARTVIEW   19979  E     1       [17:50:55] 31/5/2019   N    SmartView
INDEXER     20032  E     1       [17:50:55] 31/5/2019   N    /opt/CPrt-R82/log_indexer/log_
indexer
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   N    /opt/CPSmartLog-
R82/smartlog_server
CP3DLOGD    20237  E     1       [17:50:55] 31/5/2019   N    cp3dlogd
EPM         20251  E     1       [17:50:56] 31/5/2019   N    startEngine
DASERVICE   20404  E     1       [17:50:59] 31/5/2019   N    DAService_script
[Expert@HostName:0]#
```

例 - 管理サーバの冗長出力

```
[Expert@HostName:0]# cpwd_admin list -full
APP        PID    STAT  #START  START_TIME             SLP/LIMIT  MON
-------------------------------------------------------------------------------
CPVIEWD    19738  E     1       [17:50:44] 31/5/2019   60/5       N
           PATH = /opt/CPshrd-R82/bin/cpviewd
           COMMAND = cpviewd
-------------------------------------------------------------------------------
HISTORYD   0      T     0       [17:54:44] 31/5/2019   60/5       N
           PATH = /opt/CPshrd-R82/bin/cpview_historyd
           COMMAND = cpview_historyd
-------------------------------------------------------------------------------
CPD        19730  E     1       [17:54:45] 31/5/2019   60/5       Y
           PATH = /opt/CPshrd-R82/bin/cpd
           COMMAND = cpd
-------------------------------------------------------------------------------
SOLR       19935  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R82/bin/java_solr
           COMMAND = java_solr /opt/CPrt-R82/conf/jetty.xml
-------------------------------------------------------------------------------
RFL        19951  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R82/bin/LogCore
           COMMAND = LogCore
-------------------------------------------------------------------------------
SMARTVIEW  19979  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R82/bin/SmartView
           COMMAND = SmartView
-------------------------------------------------------------------------------
INDEXER    20032  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R82/log_indexer/log_indexer
           COMMAND = /opt/CPrt-R82/log_indexer/log_indexer
-------------------------------------------------------------------------------
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPSmartLog-R82/smartlog_server
           COMMAND = /opt/CPSmartLog-R82/smartlog_server
           ENV = LANG=C
-------------------------------------------------------------------------------
CP3DLOGD   20237  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPuepm-R82/bin/cp3dlogd
           COMMAND = cp3dlogd
-------------------------------------------------------------------------------
EPM        20251  E     1       [17:50:56] 31/5/2019   60/5       N
           PATH = /opt/CPuepm-R82/bin/startEngine
           COMMAND = startEngine
-------------------------------------------------------------------------------
DASERVICE  20404  E     1       [17:50:59] 31/5/2019   60/5       N
           PATH = /opt/CPda/bin/DAService_script
           COMMAND = DAService_script
[Expert@HostName:0]#
```

cpwd_admin monitor_list

説明

アクティブモニタリング対象プロセスの状態を画面に表示します。

アクティブモニタリングについては*cpwd_admin (819ページ)*。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin monitor_list
```

例

```
[Expert@HostName:0]# cpwd_admin monitor_list
cpwd_admin:
APP        FILE_NAME                      NO_MSG_TIMES   LAST_MSG_TIME
CPD        CPD_5420_4714.mntr             0/10           [19:00:33] 31/5/2019
[Expert@HostName:0]#
```

cpwd_admin start

説明

WatchDogがモニタしているプロセスを開始します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin start -name <Application Name> -path "<Full Path to
Executable>" -command "<Command Syntax>" [-env {inherit | <Env_
Var>=<Value>] [-slp_timeout <Timeout>] [-retry_limit {<Limit> |
u}]
```

パラメータ

パラメータ	説明
-name <*Application Name*>	名前、その下にcpwd_admin listコマンドがモニタプロセスを一番左のカラムに表示します(APP) 。 例: ■ FWM ■ FWD ■ CPD ■ CPM
-path "<*Full Path to Executable*>"	実行ファイル名を含む、実行ファイルのフルパス(Check Point環境変数の有無にかかわらず) 。 二重引用符で囲む必要があります。 例: ■ FWMの場合 : "$FWDIR/bin/fwm" ■ FWDの場合 : "/opt/CPsuite-R82/fw1/bin/fw" ■ CPDの場合 : "$CPDIR/bin/cpd" ■ CPMの場合 : "/opt/CPsuite-R82/fw1/scripts/cpm.sh" ■ SICTUNNELの場合 : "/opt/CPshrd-R82/bin/cptnl"

パラメータ	説明
`-command "<Command Syntax>"`	実行するコマンドとその引数。 二重引用符で囲む必要があります。 例: ■ FWMの場合: `"fwm"` ■ マルチドメインサーバでのFWMの場合: `"fwm mds"` ■ FWDの場合: `"fwd"` ■ CPDの場合: `"cpd"` ■ CPMの場合: `"/opt/CPsuite-R82/fw1/scripts/cpm.sh -s"` ■ SICTUNNELの場合: `"/opt/CPshrd-R82/bin/cptnl -c "/opt/CPuepm-R82/engine/conf/cptnl_srv.conf""`
`-env {inherit | <Env_Var>=<Value>}`	シェルから環境変数を引き継ぐかどうかを設定します。 ■ `inherit`- すべての環境変数を継承(WatchDogは最大80の環境変数をサポート) ■ `<Env_Var>=<Value>`- 指定された値を指定された環境変数に代入する
`-slp_timeout <Timeout>`	コンフィグレーションパラメータ`"sleep_timeout"`の指定値を設定します。 参照: *cpwd_admin config (822ページ)*。
`-retry_limit {<Limit> | u}`	コンフィギュレーションパラメータ`"retry_limit"`の値を設定します。 参照: *cpwd_admin config (822ページ)*。 ■ `<Limit>`- 指定された回数プロセスの再起動を試みる ■ `u`- 回数無制限でプロセスの再起動を試みる

例

プロセスのリストと適用可能な構文については、sk97638を参照してください。

cpwd_admin start_monitor

説明

アクティブなWatchDogモニタリングを開始します。WatchDogは、あらかじめ設定されたプロセスをアクティブにモニタします。

説明を参照：*cpwd_admin (819ページ)*コマンドを実行します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin start_monitor
```

例

```
[Expert@HostName:0]# cpwd_admin start_monitor
cpwd_admin:
CPWD has started to perform active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

cpwd_admin stop

説明

WatchDogがモニタしているプロセスを停止させます。

重要 - この変更は再起動後は保持され**ません**。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin stop -name <Application Name> [-path "<Full Path to Executable>" -command "<Command Syntax>" [-env {inherit | <Env_Var>=<Value>]
```

パラメータ

パラメータ	説明
`-name <Application Name>`	`cpwd_admin list`コマンドがモニタするプロセスを左端のカラムに表示する名前`APP`。 例: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-path "<Full Path to Executable>"`	実行ファイル名を含む、実行ファイルのフルパス(Check Point 環境変数の有無にかかわらず) 。 二重引用符で囲む必要があります。 例: ■ FWMの場合 : "`$FWDIR/bin/fwm`" ■ FWDの場合 : "`/opt/CPsuite-R82/fw1/bin/fw`" ■ CPDの場合 : "`$CPDIR/bin/cpd_admin`"
`-command "<Command Syntax>"`	実行するコマンドとその引数。 二重引用符で囲む必要があります。 例: ■ FWMの場合 : "`fw kill fwm`" ■ FWDの場合 : "`fw kill fwd`" ■ CPDの場合 : "`cpd_admin stop`"

パラメータ	説明
`-env {inherit | <Env_Var>=<Value>}`	シェルから環境変数を引き継ぐかどうかを設定します。 ■ `inherit`- 全ての環境変数を継承(WatchDogは最大80の環境変数をサポート) ■ `<Env_Var>=<Value>`- 指定された値を指定された環境変数に代入

例

プロセスのリストと適用可能な構文については、sk97638を参照してください。

cpwd_admin stop_monitor

説明

アクティブなWatchDogのモニタリングを停止します。WatchDogはすべてのプロセスを受動的にのみモニタします。

の説明を参照のこと。*cpwd_admin (819ページ)*コマンドを実行します。

Gaia ClishまたはエキスパートモードのManagement Serverでの構文

```
cpwd_admin stop_monitor
```

例

```
[Expert@HostName:0]# cpwd_admin stop_monitor
cpwd_admin:
CPWD has stopped performing active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

dbedit

説明

Security Management ServerまたはDomain Management Server上の管理データベース(`$FWDIR/conf/objects_5_0.C`ファイル)を編集します。sk13301を参照してください。

重要 - Check Pointのサポートまたは R&Dから明示的な指示がない限り、このコマンドを実行しないでください。管理データベースの設定が壊れる可能性があります。

構文

```
dbedit -help
```

```
dbedit [-globallock] [{-local | -s <Management_Server>}] [{-u
<Username> | -c <Certificate>}] [-p <Password>] [-f <File_Name>
[ignore_script_failure] [-continue_updating]] [-r "<Open_Reason_
Text>"] [-d <Database_Name>] [-listen] [-readonly] [-session]
```

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

パラメータ

パラメータ	説明
`-help`	一般的なヘルプを表示します。
`-globallock`	dbeditユーティリティで作業すると、管理データベースが一部ロックされます。ユーザがSmartConsoleで同時にオブジェクトを設定すると、管理データベースで問題が発生します。 このオプションは、SmartConsole、またはdbeditユーザが管理データベースで変更できないようにします。 このオプションを指定すると、dbeditコマンドが管理データベースのコピー上で実行されます。`dbedit`コマンドで変更を加え、`savedb`コマンドを実行すると、dbeditユーティリティが実際の管理データベースに変更を保存し、コミットします。
`-local`	ユーザ名/パスワードを使用せずに、localhost(127.0.0.1) に接続します。このパラメータを指定しない場合、dbeditユーティリティで接続方法を確認します。

パラメータ	説明
-s *<Management_Server>*	Security Management Server を指定します。IPアドレスまたはHostNameで指定します。 このパラメータを指定しない場合、dbeditユーティリティで接続方法を確認します。
-u *<Username>*	dbeditユーティリティがSecurity Management Serverに接続するためのユーザ名を指定します。 -s *<Management_Server>*"パラメータを指定した場合、必須のパラメータです。
-c *<Certificate>*	dbeditユーティリティがSecurity Management Serverに接続するための、ユーザ証明書ファイルを指定します。 -s *<Management_Server>*"パラメータを指定した場合、必須のパラメータです。
-p *<Password>*	dbeditユーティリティがSecurity Management Serverに接続するためのユーザのパスワードを指定します。 "-s *<Management_Server>*"、"-u *<Username>*"パラメータを指定する場合は必須パラメータです。
-f *<File_Name>*	該当するdbedit内部コマンドを含むファイルを指定します(下記の「*dbedit内部コマンド*」セクションを参照): ■ create *<object_type>* *<object_name>* ■ modify *<table_name>* *<object_name>* *<field_name>* *<value>* ■ update *<table_name>* *<object_name>* ■ delete *<table_name>* *<object_name>* ■ print *<table_name>* *<object_name>* ■ quit **注** - 各コマンドは4096文字に制限されています。
ignore_script_failure	ファイル内のdbedit内部コマンドの実行を継続し、エラーを無視します。 "-f *<File_Name>*"パラメータを指定した場合に使用できます。
-continue_updating	一部のオブジェクトで操作が失敗しても、変更されたオブジェクトの更新を継続します(エラーを無視して、スクリプトの最後にupdate_allコマンドを実行します)。 "-f *<File_Name>*"パラメータを指定した場合に使用できます。
-r "*<Open_Reason_Text>*"	データベースを読み書き可能なモード(デフォルトモード)で開く理由を指定します。

パラメータ	説明
`-d <Database_Name>`	dbeditユーティリティが接続するデータベースの名前を指定します(例えば `mdsdb`)。
`-listen`	dbeditユーティリティは、変更を「リッスン」します(このモードは、Check Pointサポートの支援を受け高度なトラブルシューティングを行う場合に使用します)。 dbeditユーティリティは、管理データベースに変更が生じたときに、その内部メッセージを表示します。
`-readonly`	管理データベースを読み取り専用で開くことを指定します。
`-session`	セッションの接続性。

dbedit内部コマンド

注 - 利用可能なテーブル、クラス名(オブジェクトタイプ)、属性、値を確認するには、データベースツール(GuiDBEdit Tool)を使用して管理サーバに接続します(sk13009を参照)。

コマンド	解説、構文、例文
`-h`	**説明:** 一般的なヘルプを表示します。 **構文:** `dbedit> -h`

コマンド	解説、構文、例文

`-q`
 	
`quit`
	説明:
	dbeditを終了します。
	構文:
	`dbedit> -q`
	`dbedit> quit [-update_all | -noupdate]`
	例:
	■ ユーティリティを終了し、残りの修正オブジェクトをコミットします(インタラクティブモード)。
	`dbedit> quit`
	■ ユーティリティを終了し、残りの変更されたオブジェクトをすべて更新します。
	`dbedit> quit -update_all`
	■ ユーティリティを終了し、変更した内容をすべて破棄します。
	`dbedit> quit -no_update`

`update`	**説明:**
	指定したオブジェクトを指定したテーブルに保存します (例: "`network_objects`", "`services`", "`users`")。
	構文:
	`dbedit> update <table_name> <object_name>`
	例:
	オブジェクト *My_Service*を*services*テーブルに保存します:
	`dbedit> update services My_Service`

`update_all`	**説明:** 変更したオブジェクトをすべて保存します。 **構文:** `dbedit> update_all`

コマンド	解説、構文、例文

`_print_set`	**説明:**
	指定されたテーブル (例えば "`network_objects`", "`services`", "`users`") から、指定されたオブジェクトを`$FWDIR/conf/objects_5_0.C`ファイル (属性のセット) に表示されるように表示します。
	構文:
	`dbedit> _print_set <table_name> <object_name>`
	例:
	*network_objects*テーブルから*My_Obj*オブジェクトを表示します:
	`dbedit> print network_objects My_Obj`

`print`	**説明:**
	指定されたオブジェクトの属性の一覧を指定されたテーブルから出力します (例: "`network_objects`", "`properties`", "`services`", "`users`")。
	構文:
	`dbedit> print <table_name> <object_name>`
	例:
	■ *network_objects*テーブルからオブジェクト *My_Obj*を表示します (Network Objects) :
	`dbedit> print network_objects my_obj`
	■ *properties*テーブル(「グローバルプロパティ」) からオブジェクト *firewall_properties*を表示します:
	`dbedit> print properties firewall_properties`

コマンド	解説、構文、例文

printxml	**説明:**
	指定されたオブジェクトの属性のリストを、指定のテーブルからXML形式で出力します (例: "network_objects"、"properties"、"services"、"users")。
	Management Serverの設定をXMLファイルにエクスポートして、後で外部の自動システムで使用することができます。
	構文:
	`dbedit> printxml <table_name> [<object_name>]`
	例:
	■ *network_objects*テーブルから*My_Obj*オブジェクトを表示します:
	`dbedit> printxml network_objects my_obj`
	■ *properties*テーブル(「グローバルプロパティ」) からオブジェクト *firewall_properties*を表示します:
	`dbedit> printxml properties firewall_ properties`

printbyuid	**説明:**
	UIDで指定されたオブジェクトの属性を表示します
	(`$FWDIR/conf/objects_5_0.C`ファイルでは、オブジェクトの先頭に "`chkpf_uid ({...})`"として表示されます) 。
	構文:
	`dbedit> printbyuid {object_id}`
	例:
	指定されたUIDを持つオブジェクトの属性を表示します。
	`dbedit> printbyuid {D3833F1D-0A58-AA42-865F-39BFE3C126F1}`

コマンド	解説、構文、例文

query	**説明:**
	指定されたテーブル内のすべてのオブジェクトを表示します。
	オプションとして、特定の属性と値を持つオブジェクトを検索することができます。検索は"query <table_name>"の後にカンマで区切って行います(<*attribute*>と'<*value*>'の間にスペースは使用できません)。
	構文:
	`dbedit> query <table_name> [ , <attribute>='<value>' ]`
	例:
	■ テーブルユーザ内のすべてのオブジェクトを表示します:
	`dbedit> query users`
	■ *network_objects*テーブル内の、管理サーバとして定義されているすべてのオブジェクトを表示します:
	`dbedit> query network_objects, management='true'`
	■ *ssh*という名前を持つテーブル*サービス*内のすべてのオブジェクトを表示します:
	`command_sdbedit> query services, name='ssh'`
	■ ポート*22*を持つテーブル*サービス*内のすべてのオブジェクトを表示します:
	`dbedit> query services, port='22'`
	■ IPアドレス*10.10.10.10*を持つすべてのオブジェクトを表示します:
	`dbedit> query network_objects, ipaddr='10.10.10.10'`

whereused	**説明:**
	指定されたオブジェクトがデータベース内のどこで使用されているかを確認します。
	このオブジェクトが使用されている場所の数とその場所の関連情報を表示します。
	構文:
	`dbedit> whereused <table_name> <object_name>`
	例:
	*My_Obj*オブジェクトが使用されている場所をチェックします:
	`dbedit> whereused network_objects My_Obj`

コマンド	解説、構文、例文

`create`	**説明:**
	指定されたタイプ(デフォルト値) のオブジェクトをデータベースに作成します。
	オブジェクトの名前には制限が適用されます。
	■ オブジェクト名は最大100文字までです。
	■ オブジェクト名には、ASCII文字、数字、ダッシュのみ使用できます。
	■ 予約語はManagement Serverによってブロックされます(sk40179参照) 。
	構文:
	`dbedit> create <object_type> <object_name>`
	例:
	*tcp_service*タイプ(デフォルト値) のサービスオブジェクト *My_Service*を作成します:
	`dbedit> create tcp_service my_service`

`delete`	**説明:**
	指定されたテーブルからオブジェクトを削除します。
	構文:
	`dbedit> delete <table_name> <object_name>`
	例:
	テーブル*services*からサービスオブジェクト *My_Service*を削除します:
	`dbedit> delete services my_service`

コマンド	解説、構文、例文

`modify`	**説明:**
	管理データベースの指定されたテーブル(例: "`network_objects`"、"`services`"、"`users`")の指定されたオブジェクトの指定された属性の値を変更します。
	構文:
	`dbedit> modify <table_name> <object_name> <field_name> <value>`
	例:
	■ *services*テーブルの*My_Service*オブジェクトの色を*赤*に変更します:
	`dbedit> modify services My_Service color red`
	■ オブジェクト*MyObj*にコメントを追加します:
	`dbedit> modify network_objects MyObj comments "Created by fwadmin with dbedit"`
	■ テーブル*プロパティ*のグローバルプロパティ*ike_use_largest_possible_subnets*の値を*false*に設定します:
	`dbedit> modify properties firewall_properties ike_use_largest_possible_subnets false`
	■ セキュリティゲートウェイ*My_FW*上に新しいインタフェースを作成し、その属性を変更します - IPアドレス/マスクを設定し、*"Element Index"=3*のインタフェースでアンチスプーフィングを有効にします(データベースツール(GuiDBEditツール) でオブジェクト*My_FW*の属性を確認します(sk13009を参照)) :

コマンド	解説、構文、例文
	``` dbedit> addelement network_objects My_FW interfaces interface dbedit> modify network_objects My_FW interfaces:3:officialname NAME_OF_INTERFACE dbedit> modify network_objects My_FW interfaces:3:ipaddr IP_ADDRESS dbedit> modify network_objects My_FW interfaces:3:netmask NETWORK_MASK dbedit> modify network_objects My_FW interfaces:3:security:netaccess:access specific dbedit> modify network_objects My_FW interfaces:3:security:netaccess:allowed network_objects:group_name dbedit> modify network_objects My_FW interfaces:3:security:netaccess:perform_anti_ spoofing true dbedit> modify network_objects MyObj FieldA LINKSYS ``` ■ 所有オブジェクト *MyObj*で、*フィールドB*の値を*NewVal*に変更します: ``` dbedit> modify network_objects MyObj FieldA:FieldB NewVal ``` ■ リンクされたオブジェクト *MyObj*で、*フィールドA*の値を*B*から*C*に変更します: ``` dbedit> modify network_objects MyObj FieldA B:C ```

コマンド	解説、構文、例文

`lock`	**説明:**
	指定されたテーブル (例: "`network_objects`"、"`services`"、"`users`") の指定されたオブジェクト (管理者) を、他のユーザが変更できないようにロックします。
	例えば、リモートコンピュータから*admin1*でこの管理サーバに接続し、オブジェクトをロックした場合、*admin2*で接続することはできますが、*admin1*がロックを解除するまで、ロックされたオブジェクトを変更することはできません。
	構文:
	`dbedit> lock <table_name> <object_name>`
	例:
	データベースの*services*テーブルにある*My_Service_Obj*オブジェクトをロックします:
	`dbedit> lock services My_Service_Obj`

`addelement`	**説明:**
	指定されたテーブルの指定されたオブジェクトに、指定された複数のフィールド / コンテナ(指定された値を持つ) を追加します。
	構文:
	`dbedit> addelement <table_name> <object_name> <field_name> <value>`
	例:
	■ テーブル*ldap*のオブジェクト*My_Obj*の複数フィールド*Read*に、値*Organization*を持つエレメント*BranchObjectClass*を追加します:
	`dbedit> addelement ldap My_Obj Read:BranchObjectClass Organization`
	■ テーブル*services*のサービスグループ*MyServicesGroup*にサービス*MyService*を追加します:
	`dbedit> addelement services MyServicesGroup '' services:MyService`
	■ テーブル*network_objects*のネットワークグループ*MyNetworksGroup*にネットワーク*MyNetwork*を追加します:
	`dbedit> addelement network_objects MyNetworksGroup '' network_objects:MyNetwork`

コマンド	解説、構文、例文

rmelement	**説明:**
	指定されたテーブルの特定のオブジェクトから、特定の複数フィールド/コンテナ(指定された値を持つ) を削除します。
	構文:
	`dbedit> rmelement <table_name> <object_name> <field_name> <value>`
	例:
	■ サービスグループ*MyServicesGroup*からサービス*MyService*をテーブル*services*から削除します:
	`dbedit> rmelement services MyServicesGroup '' services:MyService`
	■ テーブル*network_objects*からネットワークグループ*MyNetworksGroup*からネットワーク*MyNetwork*を削除します:
	`dbedit> rmelement network_objects MyNetworksGroup '' network_objects:MyNetwork`
	■ テーブル*ldap*のオブジェクト*My_Obj*の複数フィールド*Read*から、値*Organization*を持つエレメント*BranchObjectClass*を削除します:
	`dbedit> rmelement ldap my_obj Read:BranchObjectClass Organization`

rename	**説明:**
	指定されたテーブルの特定のオブジェクトの名前を変更します。
	構文:
	`dbedit> rename <table_name> <object_name> <new_object_name>`
	例:
	*network_objects*テーブルのネットワークオブジェクト*london*の名前を*chicago*に変更します:
	`dbedit> rename network_objects london chicago`

コマンド	解説、構文、例文

rmbyindex	**説明:**
	エレメントのインデックスに基づいてコンテナからエレメントを削除します。
	構文:
	`dbedit> rmbyindex <table_name> <object_name> <field_name> <index_number>`
	例:
	*network_objects*テーブルのエレメントインデックス*1*のコンテナ*log_servers*から、エレメント*backup_log_servers*を削除します:
	`dbedit> rmbyindex network_objects g log_ servers:backup_log_servers 1`

add_owned_ remove_name	**説明:**
	指定された所有オブジェクトのフィールド(またはコンテナ)に、所有オブジェクトを追加(およびその名前を削除)します。
	構文:
	`dbedit> add_owned_remove_name <table_name> <object_name> <field_name> <value>`
	例:
	所有オブジェクトフィールド(またはコンテナ) *my_external_products*に所有オブジェクト*My_Gateway*を追加(およびその名前を削除)します:
	`dbedit> add_owned_remove_name network_objects My_ Gateway additional_products owned:my_external_ products`

is_delete_ allowed	**説明:**
	特定のオブジェクトが指定されたテーブルから削除可能かどうか確認します(他のオブジェクトで使用されている場合は削除できません)。
	構文:
	`dbedit> is_delete_allowed <table_name> <object_ name>`
	例:
	`dbedit> is_delete_allowed network_objects MyObj`
	オブジェクト*MyObj*を*network_objects*テーブルから削除できるかどうかを調べます:

コマンド	解説、構文、例文

`set_pass`	**説明:**
	特定のユーザに対して、指定したパスワードを設定します。
	注:
	■ パスワードは、最低4文字、最大50文字までです。
	■ このコマンドでは、管理者のパスワードを変更することはできません。
	構文:
	`dbedit> set_pass <Username> <Password>`
	例:
	ユーザ*abcd*にパスワード *1234*を設定します:
	`dbedit> set_pass abcd 1234`

`savedb`	**説明:** データベースを保存します。このコマンドは、データベースがグローバルにロックされている時 ("`dbedit -globallock`"コマンドでdbeditユーティリティを起動した時) だけ実行できます。 **構文:** `dbedit> savedb`
`savesession`	**説明:** セッションを保存します。このコマンドは、dbeditユーティリティをセッションモード ("`dbedit -session`"コマンドで) で起動したときのみ実行できます。 **構文:** `dbedit> savesession`

fw

説明

- セキュリティログや監査ログに対して様々な操作を行います。
- 指定したCheck Pointのプロセスを終了させます。
- Suspicious Activity Monitoring (SAM)ルールを管理します。
- Suspicious Activity Policyエディタを管理します。

構文

```
fw [-d]
      fetchlogs <options>
      hastat <options>
      kill <options>
      log <options>
      logswitch <options>
      lslogs <options>
      mergefiles <options>
      repairlog <options>
      sam <options>
      sam_policy <options>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`fetchlogs <options>`	特定のCheck Pointコンピュータから、特定のCheck Pointログファイル(セキュリティ(`$FWDIR/log/*.log*`)または監査(`$FWDIR/log/*.adtlog*`))を取得します。 参照: *fw fetchlogs (858ページ)*。
`hastat <options>`	ハイアベイラビリティ構成のCheck Pointコンピュータとその状態についての情報を表示します。 参照: *fw hastat (861ページ)*。

パラメータ	説明
`kill <options>`	指定されたCheck Pointのプロセスを終了します。 参照: *fw kill (862ページ)*。
`log <options>`	Check Pointの、セキュリティ(`$FWDIR/log/*.log`) または監査 (`$FWDIR/log/*.adtlog`)ログファイルの内容を表示します。 参照: *fw log (863ページ)*。
`logswitch <options>`	現在アクティブなCheck Pointのセキュリティ(`$FWDIR/log/fw.log`) または監査(`$FWDIR/log/fw.adtlog`)ログファイルを切り替えます。 参照: *fw logswitch (873ページ)*。
`lslogs <options>`	ローカルコンピュータまたはリモートコンピュータにある Check Pointのログファイル - セキュリティ(`$FWDIR/log/*.log*`) または監査 (`$FWDIR/log/*.adtlog*`) - の一覧を表示します。 参照: *fw lslogs (877ページ)*。
`mergefiles <options>`	複数のCheck Pointログファイル(セキュリティ(`$FWDIR/log/*.log`) または監査(`$FWDIR/log/*.adtlog`)) を単一のログファイルに統合します。 参照: *fw mergefiles (880ページ)*。
`repairlog <options>`	Check Pointのログファイル(セキュリティ(`$FWDIR/log/*.log`) または監査 (`$FWDIR/log/*.adtlog`)) のポインタファイルを再構築します。 参照: *fw repairlog (883ページ)*。
`sam <options>`	Suspicious Activity Monitoring (SAM)ルールを管理します。 参照: *fw sam (885ページ)*。
`sam_policy <options>` または `samp <options>`	この種のルールで動作するSuspicious Activity Policyエディタを管理します。 ■ Suspicious Activity Monitoring (SAM)ルール。 ■ レート制限ルール。 参照: *fw sam_policy (894ページ)*。

fw fetchlogs

説明

指定したCheck Pointサーバから、指定したセキュリティログファイル(`$FWDIR/log/*.log*`) または監査ログファイル(`$FWDIR/log/*.adtlog*`) を取得します。

重要:

- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。

構文

```
fw [-d] fetchlogs [-f <Name of Log File 1>] [-f <Name of Log File 2>]... [-f <Name of Log File N>] <Target>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-f <Name of Log File N>`	取得するログファイルの名前を指定します。名前のみ指定する必要があります。 **注：** ■ ログファイル名を明示的に指定しない場合、このコマンドはすべてのセキュリティログファイル(`$FWDIR/log/*.log*`)とすべての監査ログファイル(`$FWDIR/log/*.adtlog*`)を転送します。 ■ 指定したログファイル名には、ワイルドカードの*と?を含めることができます(例：`2017-0?-*.log`)。 ワイルドカードを入力する場合は、二重引用符または一重引用符で囲む必要があります。 ■ 1つのコマンドで複数のログファイルを指定することができます。 各ログファイル名パターンには、`-f`パラメータを使用する必要があります。 ■ このコマンドは、該当するログポインタファイルも転送します。
`<Target>`	このローカルCheck PointサーバがSIC信頼を確立しているリモートのCheck Pointサーバを指定します。 ■ このコマンドをSecurity Management Serverまたはドメイン管理サーバで実行する場合は、`<Target>`に該当するオブジェクト名またはSmartConsoleで設定されているCheck PointサーバのメインIPアドレスを指定します。 ■ Security Gatewayまたはクラスタメンバでこのコマンドを実行する場合、`<Target>`はSmartConsoleで設定された該当オブジェクトのメインIPアドレスになります。

注:

- このコマンドは、指定したCheck Pointサーバの`$FWDIR/log/`ディレクトリから指定したログファイルを移動します。つまり、コピーに成功すると、指定したCheck Pointサーバ上の指定したログファイルが削除されます。
- このコマンドは、指定したログファイルを、このコマンドを実行したローカルCheck Point サーバの`$FWDIR/log/`ディレクトリに移動します。
- このコマンドは、*アクティブな*ログファイル`$FWDIR/log/fw.log`または`$FWDIR/log/fw.adtlog`をフェッチすることはできません。

  アクティブなログファイルを取得するには

  1. 該当するCheck Pointサーバでログスイッチを実行します:

     ```
     fw logswitch [-audit] [-h <IP Address or Hostname>]
     ```

  2. 該当するCheck Pointサーバからローテートされたログファイルを取得します:

     ```
     fw fetchlogs -f <Log File Name> <IP Address or Hostname>
     ```

- このコマンドは、指定したCheck Pointサーバから取得したログファイルの名前を変更します。新しいログファイル名は、Check Pointのサーバ名(SmartConsoleで設定)、アンダースコア(_)2文字、および元のログファイル名(例:`MyGW__2019-06-01_000000.log`)を結合したものになります。

例 - 管理サーバからログファイルを取得する場合

```
[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      5796KB 2019-06-01_000000.log
      4610KB fw.log
[Expert@HostName:0]#

[Expert@HostName:0]# fw fetchlogs -f 2019-06-01_000000 MyGW
File fetching in process. It may take some time...
File MyGW__2019-06-01_000000.log was fetched successfully
[Expert@HostName:0]#

[Expert@HostName:0]# ls $FWDIR/log/MyGW*
/opt/CPsuite-R82/fw1/log/MyGW__2019-06-01_000000.log
/opt/CPsuite-R82/fw1/log/MyGW__2019-06-01_000000.logaccount_ptr
/opt/CPsuite-R82/fw1/log/MyGW__2019-06-01_000000.loginitial_ptr
/opt/CPsuite-R82/fw1/log/MyGW__2019-06-01_000000.logptr
[Expert@HostName:0]#

[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      4610KB fw.log
[Expert@HostName:0]#
```

fw hastat

説明

ハイアベイラビリティ構成のCheck Pointコンピュータとその状態についての情報を表示します。

注 - これは古いコマンドです。管理サーバで*cpstat (809ページ)*コマンドを実行します。

構文

```
fw hastat [<Target1>] [<Target2>] ... [<TargetN>]
```

パラメータ

パラメータ	説明
<ターゲット 1> <ターゲット 2> ... <ターゲット N>	照会するCheck Pointコンピュータを指定します。 管理サーバでこのコマンドを実行する場合は、該当するIPアドレス、または管理対象のSecurity GatewayまたはクラスタメンバのHostNameを入力できます。 ターゲットを指定しない場合、コマンドはローカルコンピュータに問い合わせを行います。

例 - 管理サーバからのクラスタメンバのクエリ

```
[Expert@MGMT:0]# fw hastat 192.168.3.52
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.52 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#
```

fw kill

説明

指定したCheck Pointのプロセスを終了させます。

重要:

- 終了したプロセスが再起動されていることを確認するか、手動で再起動します。sk97638を参照してください。
- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。

構文

```
fw [-d] kill [-t <Signal Number>] <Name of Process>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-t <Signal Number>`	Check Pointプロセスに送信するシグナルを指定します。 利用可能なシグナルとその番号のリストは、`kill -l`コマンドを実行してください。 シグナルについては、`kill`および`signal`のマニュアルページを参照してください。 信号を明示的に指定しない場合、コマンドは信号 15 (`SIGTERM`) を送信します。 **注** - プロセスはいくつかのシグナルを無視することができます。
`<Name of Process>`	終了せるCheck Pointプロセスの名前を指定します。 プロセス名を確認するには、`ps auxwf`コマンドを実行します。

例

```
fw kill fwd
```

fw log

説明

Check Pointの、セキュリティ(`$FWDIR/log/*.log`) または監査 (`$FWDIR/log/*.adtlog`)ログファイルの内容を表示します。

重要:

- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。

構文

```
fw log {-h | -help}
```

```
fw [-d] log [-a] [-b "<Start Timestamp>" "<End Timestamp>"] [-c <Action>] [{-f | -t}] [-g] [-H] [-h <Origin>] [-i] [-k {<Alert Name> | all}] [-l] [-m {initial | semi | raw}] [-n] [-o] [-p] [-q] [-S] [-s "<Start Timestamp>"] [-e "<End Timestamp>"] [-u <Unification Scheme File>] [-w] [-x <Start Entry Number>] [-y <End Entry Number>] [-z] [-#] [<Log File>]
```

パラメータ

パラメータ	説明
`{-h | -help}`	ビルトインの使用状況を表示します。 **注** - 組み込みの使用では、この表に記載されているパラメータのいくつかが表示されません。
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-a`	アカウントログエントリのみを表示します。

パラメータ	説明
-b "<*Start Timestamp*>" "<*End Timestamp*>"	指定した開始時刻と終了時刻の間にログに記録されたエントリのみを表示します。 ■ <*Start Timestamp*>と<*End Timestamp*>は、日付、時刻、またはその両方を指定することができます。 ■ 日付を省略した場合、コマンドでは現在の日付を想定します。 ■ <*Start Timestamp*>" と"<*End Timestamp*>は、二重引用符または一重引用符で囲む必要があります(-b 'XX' 'YY"または-b "XX" "YY) 。 ■ "-b"パラメータは、"-s"または"-e"パラメータと一緒に使用することはできません。 ■ 下記の日付と時刻のフォーマットを参照してください。
-c <*Action*>	指定されたアクションを持つイベントのみを表示します。いずれかの方法を実行します。 ■ accept ■ drop ■ reject ■ encrypt ■ decrypt ■ vpnroute ■ keyinst ■ authorize ■ deauthorize ■ authcrypt ■ ctl **注:** ■ fw logコマンドは、常にControl (ctl) のアクションを表示します。 ■ *ログインアクション*には、authcryptを使います。
-e "<*End Timestamp*>"	指定した時間以前にログに記録されたエントリのみを表示します。 **注:** ■ <*End Timestamp*>は、日付、時間、またはその両方にすることができます。 ■ <*End Timestamp*>は一重引用符または二重引用符で囲む必要があります (-e '...'または-e "...")。 ■ "-e"パラメータと"-b"パラメータを併用することはできません。 ■ 下記の日付と時刻のフォーマットを参照してください。

パラメータ	説明
`-f`	次のパラメータ: 1. 指定した条件に合致する保存されたエントリを表示します。 2. このコマンドは、現在開いているログファイルの終わりまで達した後も、ログファイルを無限に監視し続け、指定された条件に一致する新しいエントリを表示します。 **注** - アクティブなログファイルのみに適用される`$FWDIR/log/fw.log`または`$FWDIR/log/fw.adtlog`
`-g`	区切り文字を表示しません。 デフォルトの動作は ■ フィールド名の後にコロン(:)を表示する ■ フィールド値の後にセミコロン(;)を表示する
`-H`	High Level Logのキーを表示します。
`-h <Origin>`	指定したIPアドレスまたはオブジェクト名(SmartConsoleで設定)のSecurity Gatewayで生成されたログのみを表示します。
`-i`	ログのUIDを表示します。
`-k {<Alert Name> | all}`	特定のアラートタイプに一致するエントリを表示します。 ■ *<Alert Name>*- 特定のアラートタイプに一致するエントリのみを表示します: • `alert` • `mail` • `snmp_trap` • `spoof` • `user_alert` • `user_auth` ■ `all`- すべてのアラートタイプに一致するエントリーを表示する(デフォルト)。
`-l`	各ログエントリの日付と時刻の両方を表示します。 デフォルトでは、関連するエントリの上に一度だけ日付を表示し、その後、各ログエントリに時間を指定するようになっています。

パラメータ	説明
-m	ログ統一モードを指定します。 ■ initial- ログエントリの完全な統一。コマンドは、各IDに対して1つの統一ログエントリを表示します。これはデフォルトです。-fパラメータも指定した場合、出力には更新は表示されず、新規接続の開始に関連するエントリのみが表示されます。アップデートを表示するには、semiパラメータを使用します。 ■ semi- ログエントリを段階的に統一。各ログエントリに対して、以前に同じIDを持つエントリがあった場合は同一ログを統一してエントリを表示します。 ■ raw- ログを統一しない。出力には、すべてのログエントリが表示されます。
-n	ログファイル内のIPアドレスのDNS解決を行わない(これはデフォルトの動作です) 。 これにより、ログの処理が大幅に高速化されます。
-o	詳細ログチェーンを表示 - ログエントリのすべてのログセグメントを表示します。
-p	ログファイル内のポート番号の解決を行わない(これはデフォルトの動作です) 。 これにより、ログの処理が大幅に高速化されます。
-q	ログヘッダフィールドの名称を表示します。
-S	連続番号を表示します。
-s "<*Start Timestamp*>"	指定した時間以降にログに記録されたエントリのみを表示します。 **注:** ■ <*Start Timestamp*>は、日付、時間、またはその両方にすることができます。 ■ 日付を省略した場合、コマンドは現在の日付を想定します。 ■ <*Start Timestamp*>は一重引用符または二重引用符で囲む必要があります (-s '...'または-s "...")。 ■ "-s"パラメータと"-b"パラメータを併用することはできません。 ■ 下記の日付と時刻のフォーマットを参照してください。

パラメータ	説明
-t	次のパラメータ: 1. 指定した条件に合致する保存されたエントリを表示しません。 2. このコマンドは、現在開いているログファイルの終わりまで達した後も、ログファイルを無限に監視し続け、指定された条件に一致する新しいエントリを表示します。 **注** - アクティブなログファイルのみに適用される$FWDIR/log/fw.logまたは$FWDIR/log/fw.adtlog
-u <*Unification Scheme File*>	ログ統一スキームファイルのパスと名前を指定します。 デフォルトのログ統一スキームファイル: $FWDIR/conf/log_unification_scheme.C
-w	各ログエントリのフラグ(ログの「性質」を指定するために使用される異なるビット - 例えば、制御、監査、会計、補完など) を表示します。
-x <*Start Entry Number*>	ログファイルの先頭から数えて、指定したログエントリ番号以下のエントリのみを表示します。
-y <*End Entry Number*>	ログファイルの先頭から数えて、指定したログエントリ番号までのエントリのみを表示します。
-z	エラー(フィールドの値が間違っているなど) が発生した場合、ログエントリを表示し続けます。 デフォルトの動作は停止です。
-#	機密ログを平文で表示します。
<*Log File*>	読み込むログファイルを指定します。 ログファイルを明示的に指定しない場合、コマンドは$FWDIR/log/fw.logのログファイルを開きます。 切り替えられたログファイルを指定することができます。

日付と時刻のフォーマット

タイムスタンプの一部	フォーマット	例
日付のみ	`MMM DD, YYYY`	`June 11, 2018`
時間のみ 注 - この場合、コマンドは現在の日付を想定しています。	`HH:MM:SS`	`14:20:00`
日付と時刻	`MMM DD, YYYY HH:MM:SS`	`June 11, 2018 14:20:00`

出力

各出力行は1つのログエントリからなり、そのフィールドはこのようなフォーマットで表示されます。

注 - 表示されるフィールドは、接続タイプによって異なります。

```
HeaderDateHour ContentVersion HighLevelLogKey Uuid SequenceNum
Flags Action Origin IfDir InterfaceName LogId ...
```

この表は、いくつかのフィールドを説明しています。

フィールドヘッダ	説明	例
`HeaderDateHour`	日付と時刻	`12Jun2018 12:56:42`
`ContentVersion`	バージョン	`5`
`HighLevelLogKey`	ハイレベルログキー	`<max_null>`または空
`Uuid`	ログUUID	`(0x5b1f99cb,0x0,0x3403a8c0,0xc0000000)`
`SequenceNum`	ログシークエンス番号	`1`
`Flags`	ログの「性質」を指定する内部フラグ(例 : 制御、監査、会計、補完など)	`428292`

フィールドヘッダ	説明	例
Action	この接続で実行されたアクション	■ accept ■ dropreject ■ encrypt ■ decrypt ■ vpnroute ■ keyinst ■ authorize ■ deauthorize ■ authcrypt ■ ctl
Origin	このログを生成したセキュリティゲートウェイのオブジェクト名	MyGW
IfDir	インタフェースを介したトラフィックの方向性: ■ <- アウトバウンド (セキュリティゲートウェイから送信) ■ >- インバウンド (セキュリティゲートウェイで受信)	■ < ■ >

フィールドヘッダ	説明	例
InterfaceName	このトラフィックが記録されたSecurity Gatewayのインタフェース名 セキュリティゲートウェイが何らかの内部アクション(例えば、ログスイッチ)を実行した場合、ログエントリには次のように表示されます。 daemon	■ eth0 ■ daemon ■ N/A
LogId	ログID	0
Alert	アラートタイプ	■ alert ■ mail ■ snmp_trap ■ spoof ■ user_alert ■ user_auth
OriginSicName	このログを生成したセキュリティゲートウェイのSIC名	CN=MyGW,O=MyDomain_ Server.checkpoint.com.s6t98x
inzone	インバウンドセキュリティゾーン	Local
outzone	アウトバウンドセキュリティゾーン	External

フィールドヘッダ	説明	例
service_id	この接続を検査するために使用されるサービスの名前	ftp
src	接続元のコンピュータのオブジェクト名またはIPアドレス	MyHost
dst	接続先のコンピュータのオブジェクト名またはIPアドレス	MyFTPServer
proto	接続プロトコルの名前	tcp
sport_svc	接続元ポート	64933
ProductName	このログを生成したCheck Point製品の名前	■ VPN-1 & FireWall-1 ■ Application Control ■ FloodGate-1
ProductFamily	このログを生成したCheck Point製品ファミリ名	Network

例

例1 - すべてのログエントリを、各ログエントリの日付と時刻の両方で表示する

```
fw log -l
```

例2 - 指定されたタイムスタンプ以降に開始するすべてのログエントリを表示する

```
[Expert@MyGW:0]# fw log -l -s "June 12, 2018 12:33:00"
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

... ... ...

[Expert@MyGW:0]#
```

例3 - 指定されたタイムスタンプの間のすべてのログエントリを表示する

```
[Expert@MyGW:0]# fw log -l -b "June 12, 2018 12:33:00" 'June 12, 2018 12:34:00'
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

 12Jun2018 12:33:45 5 N/A 1 ctl MyGW > LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; description: Contracts; reason: Could not reach
"https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy configuration on the gateway.; Severity: 2;
status: Failed; version: 1.0; failure_impact: Contracts may be out-of-date; update_service: 1; ProductName: Security
Gateway/Management; ProductFamily: Network;
[Expert@MyGW:0]#
```

例4 - "drop"アクションを持つすべてのログエントリを表示する

```
[Expert@MyGW:0]# fw log -l -c drop
 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;
[Expert@MyGW:0]#
```

例5 - アクション "drop"を持つすべてのログエントリを表示し、すべてのフィールドヘッダを表示し、ログフラグを表示する

```
[Expert@MyGW:0]# fw log -l -q -w -c drop
 HeaderDateHour: 12Jun2018 12:33:39; ContentVersion: 5; HighLevelLogKey: <max_null>; LogUid: ; SequenceNum: 1; Flags: 428292;
Action: drop; Origin: MyGW; IfDir: <; InterfaceName: eth0; Alert: ; LogId: 0; ContextNum: <max_null>; OriginSicName:
CN=MyGW,O=MyDomain_Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer;
proto: tcp; UP_match_table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name:
MyPolicy Network; rule_uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_
table: TABLE_START; ROW_START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp;
sport_svc: 64933; ProductFamily: Network;
[Expert@MyGW:0]#
```

例6 - ログファイルの先頭から数えて0から10までのログエントリだけを表示する

```
[Expert@MyGW:0]# fw log -l -x 0 -y 10
... ...
[Expert@MyGW:0]#
```

fw logswitch

説明

現在アクティブなログファイルを切り替えます。

1. 現在アクティブなログファイルを閉じます
2. 現在アクティブなログファイルの名前を変更します
3. 新しいアクティブなログファイルをデフォルト名で作成します。

注:

- デフォルトでは、このコマンドはアクティブなセキュリティログファイルを切り替えます。
  `$FWDIR/log/fw.log`
- アクティブな監査ログファイルの切り替えを指定できます。
  `$FWDIR/log/fw.adtlog`

重要:

- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。

構文

```
fw [-d] logswitch
       [-audit] [<Name of Switched Log>]
       -h <Target> [[+ | -]<Name of Switched Log>]
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-audit`	アクティブな監査ログファイル(`$FWDIR/log/fw.adtlog`)を切り替えることを指定します。 このパラメータは、管理サーバでのみ使用できます。

パラメータ	説明
-h <*Target*>	ログを切り替えるリモートコンピュータを指定します。 **注:** ■ ローカルコンピュータとリモートコンピュータがSICの信頼関係を確立している必要があります。 ■ リモートコンピュータには、Security Gateway、Log Server、またはHA構成のSecurity Management Serverを指定できます。 ■ リモート管理コンピュータは、SmartConsoleで設定されたメインIPアドレスまたはオブジェクト名で指定できます。
<*Name of Switched Log*>	切り替えたログファイルの名前を指定します。 **注:** ■ このパラメータを指定しない場合、デフォルトの名前になります。 <YYYY-MM-DD_HHMMSS>.log <YYYY-MM-DD_HHMMSS>.adtlog 例: *2018-03-26_174455.log* ■ スイッチログファイルの名前を指定した場合のスイッチログファイル名: <Specified_Log_Name>.log <Specified_Log_Name>.adtlog ■ 切り替えられたログに指定された名前が、既存のログファイルの名前と一致する場合、ログ切り替え操作は失敗します。 ■ 切り替えられたログファイルの指定名の最大長は230文字。
+	アクティブログをリモートコンピュータからローカルコンピュータに*コピー*します。 **注:** ■ 切り替えたログファイルの名前を指定する場合は、この+(プラス)パラメータの直後に書き込む必要があります。 ■ このコマンドは、リモートコンピュータからActive Directoryをコピーし、ローカルコンピュータの$FWDIR/log/ディレクトリに保存します。 ■ 保存されるログファイルのデフォルト名: <Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log 例: *MyGW__2018-03-26_174455.log* ■ 切り替えたログファイルの名前を指定した場合に保存されるログファイルの名前: <Gateway_Object_Name>__<Specified_Log_Name>.log ■ このコマンドでリモートコンピュータからログファイルをコピーするとき、ファイルは圧縮されます。

パラメータ	説明

-	アクティブログをリモートコンピュータからローカルコンピュータに*転送*することを指定します。
	注:
	■ このコマンドは、コピーされたアクティブログファイルをローカルコンピュータの `$FWDIR/log/` ディレクトリに保存し、リモートコンピュータの切り替えられたログファイルを削除します。
	■ 切り替えられたログファイル名を指定する場合は、この-(マイナス)パラメータの直後に書き込む必要があります。
	■ 保存されるログファイルのデフォルト名:
	`<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log`
	例: *MyGW__2018-03-26_174455.log*
	■ 切り替えたログファイルの名前を指定した場合に保存されるログファイルの名前:
	`<Gateway_Object_Name>__<Specified_Log_Name>.log`
	■ このコマンドでリモートコンピュータからログファイルを転送するとき、ファイルは圧縮されます。
	■ 別の方法として*fw fetchlogs (858ページ)*コマンドを実行します。

圧縮

このコマンドは、リモートコンピュータからログファイルを転送する際に、`gzip`コマンドでファイルを圧縮します(詳細はRFC1950 ~ RFC1952を参照) 。アルゴリズムはLZ77法のバリエーションです。圧縮率はログファイルの内容によって異なり、予測することは困難です。バイナリデータは圧縮されません。ユーザ名やURLなどのテキストデータは圧縮されます。

例 - Security Management Serverまたはセキュリティゲートウェイでアクティブなセキュリティログを切り替える

```
[Expert@MGMT:0]# fw logswitch
Log file has been switched to: 2018-06-13_182359.log
[Expert@MGMT:0]#
```

例 - Security Management Serverのアクティブな監査ログを切り替える

```
[Expert@MGMT:0]# fw logswitch -audit
Log file has been switched to: 2018-06-13_185711.adtlog
[Expert@MGMT:0]#
```

例 - 管理セキュリティゲートウェイでアクティブなセキュリティログを切り替え、切り替えたログをコピーする

```
[Expert@MGMT:0]# fw logswitch -h MyGW +
Log file has been switched to: 2018-06-13_185451.log
[Expert@MGMT:0]#
[Expert@MGMT:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R82/fw1/log/fw.log
/opt/CPsuite-R82/fw1/log/MyGW__2018-06-13_185451.log
[Expert@MGMT:0]#

[Expert@MyGW:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R82/fw1/log/fw.log
/opt/CPsuite-R82/fw1/log/2018-06-13_185451.log
[Expert@MyGW:0]#
```

fw lslogs

説明

ローカルコンピュータまたはリモートコンピュータに存在するセキュリティログファイル (`$FWDIR/log/*.log`) と監査ログファイル (`$FWDIR/log/*.adtlog`) の一覧を表示します。

重要:

- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。

構文

```
fw [-d] lslogs [-f <Name of Log File 1>] [-f <Name of Log File 2>] ... [-f <Name of Log File N>] [-e] [-r] [-s {name | size | stime | etime}] [<Target>]
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-f <Name of Log File>`	表示するログファイルの名前を指定します。名前のみ指定する必要があります。 **注:** ■ ログファイル名が明示的に指定されていない場合は、すべてのセキュリティログファイル(`$FWDIR/log/*.log`) が表示されます。 ■ ファイル名には、ワイルドカードとして`*` と`?`を含めることができます (例:`2019-0?-*`) 。ワイルドカードを入力する場合は、二重引用符または一重引用符で囲む必要があります。 ■ 1つのコマンドで複数のログファイルを指定することができます。各ログファイル名パターンには、"`-f`"パラメータを使用する必要があります。 `-f <Name of Log File 1> -f <Name of Log File 2> ... -f <Name of Log File N>`

パラメータ	説明
`-e`	詳細ファイルリストを表示します。各ログファイルについて、以下の情報が含まれています。 ■ `Size`- ログファイルとそれに関連するポインタファイルの合計サイズ ■ `Creation Time`- ログファイルが作成された時間 ■ `Closing Time`- ログファイルが閉じられた時間 ■ `Log File Name`- ファイル名
`-r`	ソート順を逆順にします(降順)。
`-s {name | size | stime | etime}`	以下のソートオプションのいずれかを使用して、ログファイルのソート順を指定します。 ■ `name`- ファイル名 ■ `size`- ファイルサイズ ■ `stime`- ログファイルが作成された時間(デフォルトのオプション) ■ `etime`- ログファイルが閉じられた時間
`<Target>`	このローカルCheck PointコンピュータがSICの信頼関係を確立しているリモートCheck Pointコンピュータを指定します。 ■ Security Management ServerまたはDomain Management Server上でこのコマンドを実行する場合、`<Target>`は該当するオブジェクトの名前、またはSmartConsoleで設定されているCheck PointコンピュータのメインIPアドレスになります。 ■ Security Gatewayまたはクラスタメンバでこのコマンドを実行する場合、`<Target>`はSmartConsoleで設定された該当オブジェクトのメインIPアドレスになります。

例1 - デフォルトの出力

```
[Expert@HostName:0]# fw lslogs
     Size Log file name
        9KB 2019-06-14_000000.log
       11KB 2019-06-15_000000.log
        9KB 2019-06-16_000000.log
       10KB 2019-06-17_000000.log
        9KB fw.log
[Expert@HostName:0]#
```

例2 - すべてのログファイルを表示する場合

```
[Expert@HostName:0]# fw lslogs -f "*"
     Size Log file name
          9KB fw.adtlog
          9KB fw.log
          9KB 2019-05-29_000000.adtlog
          9KB 2019-05-29_000000.log
          9KB 2019-05-20_000000.adtlog
          9KB 2019-05-20_000000.log
[Expert@HostName:0]#
```

例3 - パターンで指定されたログファイルのみ表示する場合

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
          9KB 2019-06-14_000000.adtlog
          9KB 2019-06-14_000000.log
         11KB 2019-06-15_000000.adtlog
         11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

例4 - パターンで指定されたログファイルとその詳細情報のみ表示する場合

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
          9KB 2019-06-14_000000.adtlog
          9KB 2019-06-14_000000.log
         11KB 2019-06-15_000000.adtlog
         11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

例5 - パターンで指定されたログファイルのみを、名前の逆順に並べて表示する場合

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' -e -s name -r
     Size Creation Time Closing Time Log file name
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.log
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.adtlog
         9KB 13Jun2018 18:23:59 14Jun2018 0:00:00 2019-06-14_000000.log
         9KB 13Jun2018 0:00:00 14Jun2018 0:00:00 2019-06-14_000000.adtlog
[Expert@HostName:0]#
```

例 6 - メインIPアドレスが192.168.3.53の管理対象 Security Gatewayから、パターンで指定されたログファイルのみ表示する場合

```
[Expert@MGMT:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' 192.168.3.53
     Size Log file name
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
         9KB 2019-06-14_000000.log
         9KB 2019-06-14_000000.adtlog
[Expert@MGMT:0]#
```

fw mergefiles

説明

複数のセキュリティログファイル(`$FWDIR/log/*.log`)を1つのログファイルにマージします。

複数の監査ログファイル(`$FWDIR/log/*.adtlog`)を1つのログファイルに統合します。

重要:

- **アクティブな**セキュリティファイル`$FWDIR/log/fw.log`を他のセキュリティ切り替えログファイルと結合しないでください。
  アクティブなセキュリティファイル`$FWDIR/log/fw.log`を切り替え(*fw logswitch (873ページ)*コマンド)、その後、他のセキュリティ切り替えログファイルとマージします。
- **アクティブな**監査ファイル`$FWDIR/log/fw.adtlog`を他の監査切り替えログファイルとマージしないでください。
  アクティブな監査ファイル`$FWDIR/log/fw.adtlog`を切り替え(*fw logswitch (873ページ)*コマンド)、その後、他の監査ログファイルとマージします。
- このコマンドは、同じUnique-ID(UID) を持つログのエントリを統一します。特定のログのすべてのセグメントが到着する前に現在のアクティブなログファイルを回転させた場合、このコマンドは2つの異なるファイルから同じユニークIDを持つレコードを1つの完全に詳細なレコードにマージします。
- 最終的にマージされるログファイルのサイズが2GBを超える場合、このコマンドはマージされたファイルのリストを作成し、各マージされたファイルのサイズが2GBを超えないようにします。
  ユーザにはこのような警告が表示されます。

  ```
  Warning: The size of the files you have chosen to merge
  is greater than 2GB. The merge will produce two or more
  files.
  ```

  マージされたファイルの名称:
  - *<Name of Merged Log File>*.log
  - *<Name of Merged Log File>*_1.log
  - *<Name of Merged Log File>*_2.log
  - ... ...
  - *<Name of Merged Log File>*_N.log

重要:

- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。

構文

```
fw [-d] mergefiles {-h | -help}
```

```
fw [-d] mergefiles [-r] [-s] [-t <Time Conversion File>] <Name of Log File 1> <Name of Log File 2> ... <Name of Log File N> <Name of Merged Log File>
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
{-h | -help}	ビルトインの使用状況を表示します。
-r	重複するエントリを削除します。
-s	マージされたファイルをログレコードのTimeフィールドでソートします。

-t <Time Conversion File>	マージ中の時間調整方法をこのコマンドに指示するファイルのフルパスと名前を指定します。
	これは、異なるタイムゾーンで設定されたログサーバからログファイルをマージする場合に必要です。
	ファイル形式:
	`<IP Address of Log Server #1>`
	`<Signed Date Time #1 in Seconds>`
	`<IP Address of Log Server #2>`
	`<Signed Date Time #2 in Seconds>`
	`... ...`
	注
	■ 絶対パスとファイル名を指定する必要があります。
	■ タイム変換ファイルの名前は、230文字以下にしてください。

パラメータ	説明
<Name of Log File 1> ... <Name of Log File N>	マージするログファイルを指定します。 **注:** ■ 入力ログファイルの絶対パスとファイル名を指定する必要があります。 ■ 入力ログファイルの名前は230文字以下にしてください。
<Name of Merged Log File>	出力されるマージされたログファイルを指定します。 **注:** ■ マージされたログファイルの名前は、230文字以下にしてください。 ■ 指定された名前のファイルがすでに存在する場合は、コマンドは停止し、既存のファイルを削除するか、別の名前を指定するかを確認します。 ■ マージされたログファイルのサイズは、2GBを超えることはできません。このような場合、コマンドはマージされた複数のログファイルを作成し、それぞれがサイズ制限を超えないようにします。

例 - セキュリティログファイルのマージ

```
[Expert@HostName:0]# ls -l $FWDIR/*.log
-rw-rw-r-- 1 admin root 189497 Sep  7 00:00 2019-09-07_000000.log
-rw-rw-r-- 1 admin root  14490 Sep  9 09:52 2019-09-09_000000.log
-rw-rw-r-- 1 admin root  30796 Sep 10 10:56 2019-09-10_000000.log
-rw-rw-r-- 1 admin root  24503 Sep 10 13:08 fw.log
[Expert@HostName:0]#
[Expert@HostName:0]# fw mergefiles -s $FWDIR/2019-09-07_000000.log $FWDIR/2019-09-09_000000.log
$FWDIR/2019-09-10_000000.log /var/log/2019-Sep-Merged.log
[Expert@HostName:0]#
[Expert@HostName:0]# ls -l /var/log/2019-Sep-Merged.log*
-rw-rw---- 1 admin root 213688 Sep 10 13:18 /var/log/2019-Sep-Merged.log
-rw-rw---- 1 admin root   8192 Sep 10 13:18 /var/log/2019-Sep-Merged.logLuuidDB
-rw-rw---- 1 admin root     80 Sep 10 13:18 /var/log/2019-Sep-Merged.logaccount_ptr
-rw-rw---- 1 admin root   2264 Sep 10 13:18 /var/log/2019-Sep-Merged.loginitial_ptr
-rw-rw---- 1 admin root   4448 Sep 10 13:18 /var/log/2019-Sep-Merged.logptr
[Expert@HostName:0]#
```

fw repairlog

説明

Check Pointセキュリティログファイル (`$FWDIR/log/*.log`) と監査ログファイル (`$FWDIR/log/*.adtlog`) はデータベースであり、特殊なポインタファイルです。

これらのログポインタファイルが破損した場合 (ログファイルが読めなくなる) 、このコマンドで再構築することができます。

ログファイルの種類	ログファイルの場所	ログポインタファイル

セキュリティログ	`$FWDIR/log/*.log`	`*.logptr`
		`*.logaccount_ptr`
		`*.loginitial_ptr`
		`*.logLuuidDB`

監査ログ	`$FWDIR/log/*.adtlog`	`*.adtlogptr`
		`*.adtlogaccount_ptr`
		`*.adtloginitial_ptr`
		`*.adtlogLuuidDB`

重要:

- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。

構文

```
fw [-d] repairlog [-u] <Name of Log File>
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。
-u	ログファイル内のユニフィケーションチェーンを再構築することを指定します。
<Name of Log File>	修復するログファイルの名前。

例 - 監査ログファイルの修復

```
fw repairlog -u 2019-06-17_000000.adtlog
```

fw sam

説明

Suspicious Activity Monitoring (SAM)ルールを管理します。SAMルールを使用すれば、セキュリティポリシーを変更したり再インストールしたりすることなく、IPアドレスへの接続やIPアドレスからの接続をブロックすることができます。詳細は、sk112061を参照してください。

Suspicious Activity Rulesは、2つの方法で作成できます。

- SmartConsoleのモニタリング結果から
- CLIで`fw sam`コマンドを使用

注:

- 詳細は*fw sam_policy (894ページ)*と*sam_alert (992ページ)*コマンドを実行。
- SAMルールは、セキュリティゲートウェイのCPUリソースを消費します。

  ベストプラクティスSAMポリシーのルールは、セキュリティゲートウェイのCPUリソースを消費します。ルールの有効期限は、調査するための時間を確保しつつ、パフォーマンスに影響を与えないように設定します。必要なSAMポリシールールだけを残しておきます。リスクがあるアクティビティを確認した場合、セキュリティポリシーの編集、ユーザへの教育など、リスクへの対応を行います。
- 強制されたSAMルール(`fw sam`コマンドで設定)のログは、`$FWDIR/log/sam.dat`ファイルに保存されます。
  保存されているエントリが10万件に達すると、ファイルが消去される設定になっています。
  このデータログファイルには、これらのいずれかの形式で記録されています。

  ```
  <type>,<actions>,<expire>,<ipaddr>
  ```

  ```
  <type>,<actions>,<expire>,<src>,<dst>,<dport>,<ip_p>
  ```
- SAM Requestsはセキュリティゲートウェイのカーネルテーブル`sam_requests`に格納されます。
- SAMルールでブロックされたIPアドレスは、セキュリティゲートウェイのカーネルテーブル`sam_blocked_ips`に格納されます。

注 - セキュリティゲートウェイまたはクラスタのSAMサーバ設定を構成するには:

1. SmartConsoleで該当するSecurity Management ServerまたはDomain Management Serverに接続します。
2. 左側のナビゲーションパネルで**Gateways & Servers**をクリックします。
3. セキュリティゲートウェイまたはクラスタのオブジェクトを開きます。
4. 左側のツリーから、**Other > SAM**をクリックします。
5. 設定を行います。
6. クリック**OK**。
7. Security Gatewayまたはクラスタオブジェクトにアクセスコントロールポリシーをインストールします。

重要:

- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- クラスタでは、すべてのクラスタメンバを同じ方法で設定する必要があります。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。
- VSNextモードと従来のVSXモードは、SAM(Suspicious Activity Monitoring) ルールをサポート**しません**。sk79700を参照してください。

構文

- **基準に従ってSAMルールを追加またはキャンセルするには:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-t <Timeout>] [-l <Log
Type>] [-C] [-e <key=val>]+ [-r] -{n|i|I|j|J} <Criteria>
```

- **すべてのSAMルールを削除するには:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] -D
```

- **すべてのSAMルールをモニタするには:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q} all
```

- **基準に従ってSAMルールをモニタするには:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q}
<Criteria>
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。

パラメータ	説明
`-v`	詳細モードを有効にします。 このモードでは、コマンドが実行されるセキュリティゲートウェイごとに、*stderr*にメッセージが1つずつ書き込まれます。これらのメッセージは、コマンドが成功したかどうかを示します。
`-s <SAM Server>`	コマンドを実行するセキュリティゲートウェイのIPアドレス(X.X.X.X形式)または解決可能なHostNameを指定します。 デフォルトは`localhost`です。
`-S <SIC Name of SAM Server>`	連絡するSAMサーバのSIC名を指定します。SAMサーバはこのSIC名を持っている必要があり、そうでない場合は接続に失敗します。 **注:** ■ SIC名を明示的に指定しない場合、SIC名の比較なしで接続が続行されます。 ■ SICの有効化に関する詳細は、OPSEC API仕様書を参照。 ■ VSX Gateway上で、*fw vsx showcs -vs <VSID>*コマンドを実行し、該当する仮想システムのSIC名を表示します。

パラメータ	説明
`-f <Security Gateway>`	アクションを実行するセキュリティゲートウェイを指定します。 *<Security Gateway>*次のいずれか: ■ *すべて* - デフォルト。SAMサーバが動作する、管理されたすべてのセキュリティゲートウェイにアクションを強制するように指定します。 この構文は、Security Management ServerまたはDomain Management Serverでのみ使用することができます。 ■ *localhost* - このローカルのCheck Pointコンピュータ(`fw sam` コマンドが実行されるコンピュータ) でアクションを実行するように指定します。 この構文は、セキュリティゲートウェイまたはStandAloneでのみ使用できます。 ■ *ゲートウェイ* - SAM サーバが実行されるセキュリティゲートウェイとして定義されたすべてのオブジェクトに対してアクションを実行するように指定します。 この構文は、Security Management ServerまたはDomain Management Serverでのみ使用することができます。 ■ *セキュリティゲートウェイオブジェクトの名前* - この特定のセキュリティゲートウェイオブジェクトにアクションを実行するように指定します。 この構文は、Security Management ServerまたはDomain Management Serverでのみ使用することができます。 ■ *グループオブジェクトの名前* - このグループオブジェクト内のすべての特定のセキュリティゲートウェイにアクションを実行するように指定します。 **注:** ■ この構文は、Security Management ServerまたはDomain Management Serverでのみ使用することができます。 ■ VSX GatewayとVSXクラスタメンバは、Suspicious Activity Monitoring (SAM) ルールをサポートしていません。sk79700を参照してください。
`-D`	すべての禁止(`"-i"`, `"-j"`, `"-I"`, `"-J"`) と通知(`"-n"`) パラメータをキャンセルします。 **注:** ■ 禁止されている接続を「解除」するには、`fw sam`コマンドに`"-C"`または`"-D"`パラメータを付けて実行します。 ■ アクティブなSAMリクエストにこのコマンドを使用することもできます。

パラメータ	説明
-C	指定されたパラメータでの接続を禁止するfw samコマンドをキャンセルします。 **注:** ■ これらの接続は、もはや阻害されません(拒否またはドロップされない)。 ■ コマンドパラメータは、-t <*Timeout*>パラメータを除き、元のfw samコマンドのパラメータと一致している必要があります。
-t <*Timeout*>	アクションを実行する時間帯(秒)を指定します。 デフォルトはforever、またはfw samコマンドをキャンセルするまでです。
-l <*Log Type*>	強制動作のログの種類を指定します。 ■ nolog- ログ/アラートの生成なし ■ short_noalert- ログの生成 ■ short_alert- アラートの発生 ■ long_noalert- ログの生成 ■ long_alert- アラートの生成(デフォルト)
-e <*key=val*>+	キーと与えられた値に基づいて、ルール情報を指定します。 複数のキーは、プラス記号(+)で区切られます。 使用可能なキーは以下のとおりです(それぞれ100文字以内)。 ■ name- セキュリティルール名 ■ comment- セキュリティルールのコメント ■ originator- セキュリティルール作成ユーザ名
-r	IPアドレスを解決しないことを指定します。
-n	通知のロングフォーマットログエントリを生成します。 **注:** ■ このパラメータは、指定されたサービスまたはIPアドレスに一致する接続がセキュリティゲートウェイを通過するときにアラートを生成します。 ■ この動作は、接続をブロック/終了するものではありません。
-i	指定されたパラメータによる新規接続を禁止(ドロップまたは拒否)します。 **注:** ■ ブロックされた各接続は、ログタイプに従ってログに記録されます。 ■ 一致する接続は拒否されます。

パラメータ	説明
`-I`	指定されたパラメータを持つ新規接続を禁止(ドロップまたは拒否)し、指定されたパラメータを持つ既存の接続をすべて閉じます。 **注:** ■ 一致する接続は拒否されます。 ■ ブロックされた各接続は、ログタイプに従ってログに記録されます。
`-j`	指定されたパラメータによる新規接続を禁止(ドロップまたは拒否)します。 **注:** ■ 一致する接続はドロップされます。 ■ ブロックされた各接続は、ログタイプに従ってログに記録されます。
`-J`	指定されたパラメータを持つ新規接続を禁止し、指定されたパラメータを持つ既存の接続をすべて閉じます。 **注:** ■ 一致する接続はドロップされます。 ■ ブロックされた各接続は、ログタイプに従ってログに記録されます。
`-b`	指定されたパラメータによる新規接続をバイパスします。
`-q`	指定されたパラメータを持つ新しい接続を隔離します。
`-M`	指定されたアクションと基準で、アクティブなSAMリクエストを監視します。
`all`	アクティブなSAMリクエストをすべて取得します。これはモニタ用としてのみ使用します。
`<Criteria>`	基準は、接続のマッチングに使用されます。 基準とは、以下のパラメータの様々な組み合わせで構成されます。 ■ 送信元IPアドレス ■ ソースネットマスク ■ 宛先 IP アドレス ■ 宛先ネットマスク ■ ポート *IANA Service Name and Port Number Registry*) ■ プロトコル番号 (*IANA Protocol Numbers*)

パラメータ	説明
	可能な組み合わせは以下のとおりです(この表の下にある説明を参照)。 ■ src <*IP*> ■ dst <*IP*> ■ any <*IP*> ■ subsrc <*IP*> <*Netmask*> ■ subdst <*IP*> <*Netmask*> ■ subany <*IP*> <*Netmask*> ■ srv <*Src IP*> <*Dest IP*> <*Port*> <*Protocol*> ■ subsrv <*Src IP*> <*Src Netmask*> <*Dest IP*> <*Dest Netmask*> <*Port*> <*Protocol*> ■ subsrvs <*Src IP*> <*Src Netmask*> <*Dest IP*> <*Port*> <*Protocol*> ■ subsrvd <*Src IP*> <*Dest IP*> <*Dest Netmask*> <*Port*> <*Protocol*> ■ dstsrv <*Dest IP*> <*Port*> <*Protocol*> ■ subdstsrv <*Dest IP*> <*Dest Netmask*> <*Port*> <*Protocol*> ■ srcpr <*IP*> <*Protocol*> ■ dstpr <*IP*> <*Protocol*> ■ subsrcpr <*IP*> <*Netmask*> <*Protocol*> ■ subdstpr <*IP*> <*Netmask*> <*Protocol*> ■ generic <*key=val*>

<*Criteria*>構文の説明

パラメータ	説明
src <*IP*>	接続元IPアドレスに一致します。
dst <IP>	接続先のIPアドレスに一致します。
any <*IP*>	接続元IPアドレスまたは接続先IPアドレスのいずれかに一致します。
subsrc <*IP*> <*Netmask*>	ネットマスクに応じた接続元IPアドレスにマッチします。
subdst <*IP*> <*Netmask*>	ネットマスクに応じた接続先IPアドレスに一致します。
subany <*IP*> <*Netmask*>	ネットマスクに応じた接続元IPアドレスまたは接続先IPアドレスのいずれかに一致します。

パラメータ	説明
`srv <Src IP> <Dest IP> <Port> <Protocol>`	特定の送信元IPアドレス、送信先IPアドレス、サービス(ポート番号)、プロトコルにマッチします。
`subsrv <Src IP> <Netmask> <Dest IP> <Netmask> <Port> <Protocol>`	特定の送信元IPアドレス、送信先IPアドレス、サービス(ポート番号)、プロトコルにマッチします。 送信元と送信先のIPアドレスは、ネットマスクに従って割り当てられます。
`subsrvs <Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>`	特定の送信元IPアドレス、送信元ネットマスク、送信先ネットマスク、サービス(ポート番号)、プロトコルにマッチします。
`subsrvd <Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>`	特定の送信元IPアドレス、宛先IP、宛先ネットマスク、サービス(ポート番号)、プロトコルに一致します。
`dstsrv <Dest IP> <Service> <Protocol>`	特定の宛先IPアドレス、サービス(ポート番号)、プロトコルにマッチします。
`subdstsrv <Dest IP> <Netmask> <Port> <Protocol>`	特定の宛先IPアドレス、サービス(ポート番号)、プロトコルにマッチします。 宛先 IP アドレスはネットマスクに応じて割り当てられます。
`srcpr <IP> <Protocol>`	送信元IPアドレスとプロトコルに一致します。
`dstpr <IP> <Protocol>`	宛先IPアドレスとプロトコルに一致します。
`subsrcpr <IP> <Netmask> <Protocol>`	接続元のIPアドレスとプロトコルにマッチします。 送信元IPアドレスは、ネットマスクに従って割り当てられます。
`subdstpr <IP> <Netmask> <Protocol>`	接続先のIPアドレスとプロトコルにマッチします。 宛先 IP アドレスはネットマスクに応じて割り当てられます。

パラメータ	説明
`generic <key=val>+`	指定されたキーと提供された値に基づいて、GTP接続をマッチングします。 複数のキーは、プラス記号 (+) で区切られます。 使用可能なキーは以下のとおりです。 ■ `service=gtp` ■ `imsi` ■ `msisdn` ■ `apn` ■ `tunl_dst` ■ `tunl_dport` ■ `tunl_proto`

fw sam_policy

説明

このタイプのルールで動作するSuspicious Activity Policyエディタを管理します。

- Suspicious Activity Monitoring (SAM)ルール。

  sk112061: How to create and view Suspicious Activity Monitoring (SAM) Rulesを参照してください。

- レート制限ルール。

  sk182350 - How to configure Rate Limiting rules for DoS Mitigationを参照してください。

また、以下のコマンドも参照してください。

- *fw sam (885ページ)*
- *sam_alert (992ページ)*

注：

- これらのコマンドは互換性があります。
  - IPv4の場合："`fw sam_policy`"および"`fw samp`"
  - IPv6の場合："`fw6 sam_policy`"および"`fw6 samp`"
- Gaia Clishまたはエキスパートモードでこれらのコマンドのいずれかを実行します。
- セキュリティゲートウェイは、SAM Policyのルールを`$FWDIR/database/sam_policy.db`ファイルに保存します。
- Security Gartner Magic Quadrant は、SAM ポリシー管理設定を`$FWDIR/database/sam_policy.mng`ファイルに保存します。

重要：

- これらのコマンドで設定した内容は、再起動後も有効になります。
- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- クラスタでは、すべてのクラスタメンバを同じ方法で設定する必要があります。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。
- VSNextモードと従来のVSXモードは、SAM(Suspicious Activity Monitoring) ルールをサポート**しません**。sk79700を参照してください。

ベストプラクティスSAMポリシーのルールは、セキュリティゲートウェイのCPUリソースを消費します。ルールの有効期限は、調査するための時間を確保しつつ、パフォーマンスに影響を与えないように設定します。必要なSAMポリシールールだけを残しておきます。リスクがあるアクティビティを確認した場合、セキュリティポリシーの編集、ユーザへの教育など、リスクへの対応を行います。

IPv4の構文

```
fw [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

IPv6の構文

```
fw6 [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw6 [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`add <options>`	レート制限のルールを1つずつ追加します。 参照: *fw sam_policy add (897ページ)*。
`batch`	一度に多くのレート制限ルールを追加または削除します。 参照: *fw sam_policy batch (911ページ)*。
`del <options>`	設定されたレート制限ルールを1つずつ削除します。 参照: *fw sam_policy del (913ページ)*。
`get <options>`	設定されているすべてのレート制限ルールを表示します。 参照: *fw sam_policy get (916ページ)*。

fw sam_policy add

説明

"fw sam_policy add"と"fw6 sam_policy add"コマンド:

- 一度に1つのSAM(Suspicious Activity Monitoring) ルールを追加します。
- 一度に1つのレート制限ルールを追加します。

注:

- これらのコマンドは互換性があります。
  - IPv4の場合: "fw sam_policy"および"fw samp"
  - IPv6の場合: "fw6 sam_policy"および"fw6 samp"
- Gaia Clishまたはエキスパートモードでこれらのコマンドのいずれかを実行します。
- セキュリティゲートウェイは、SAM Policyのルールを$FWDIR/database/sam_policy.dbファイルに保存します。
- Security Gartner Magic Quadrant は、SAMポリシー管理設定を$FWDIR/database/sam_policy.mngファイルに保存します。

重要:

- これらのコマンドで設定した内容は、再起動後も有効になります。
- このコマンドはExpertモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- クラスタでは、すべてのクラスタメンバを同じ方法で設定する必要があります。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。
- VSNextモードと従来のVSXモードは、SAM(Suspicious Activity Monitoring) ルールをサポート**しません**。sk79700を参照してください。

ベストプラクティスSAMポリシーのルールは、セキュリティゲートウェイのCPUリソースを消費します。ルールの有効期限は、調査するための時間を確保しつつ、パフォーマンスに影響を与えないように設定します。必要なSAMポリシールールだけを残しておきます。リスクがあるアクティビティを確認した場合、セキュリティポリシーの編集、ユーザへの教育など、リスクへの対応を行います。

IPv4のSAM(Suspicious Activity Monitoring) ルールを設定するための構文

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

IPv6のSAM(Suspicious Activity Monitoring) ルールを設定するための構文

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

IPv4のレート制限ルールを設定するための構文

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments>
```

IPv6のレート制限ルールを設定するための構文

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-u`	オプションです。 ルールカテゴリが`User-defined`であることを指定します。 デフォルトのルールカテゴリは`Auto`です。
`-a {d | n | b}`	必須です。 トラフィックがルール条件に一致する場合のルールアクションを指定します。 ■ `d` - 接続を切る。 ■ `n` - 接続を通知し(ログを生成) 、通過させる。 ■ `b` - 接続をバイパスする - ポリシールールと照合することなく、接続を許可。 **注** - アクションがバイパスに設定されているルールは、ログまたは制限の指定を持つことはできません。迂回したパケットと接続は、タイプ比率の制限を実施するための全体のパケット数とコネクション数にカウントされません。

パラメータ	説明
`-l {r | a}`	オプション。 このルールに一致するすべてのトラフィックに対して、どのタイプのログを生成するかを指定します。 ■ `-r`- 定期的なログの作成 ■ `-a`- 警告ログの作成
`-t <Timeout>`	オプションです。 ルールが適用される時間帯(秒)を指定します。 デフォルトのタイムアウトは無期限です。
`-f <Target>`	オプションです。 レート制限ルールを適用する対象のセキュリティゲートウェイを指定します。 `<Target>`次のいずれか: ■ `all`- これはデフォルトのオプションです。管理されているすべてのセキュリティゲートウェイでルールを実施することを指定します。 ■ セキュリティゲートウェイまたはクラスタオブジェクトの名前 - このセキュリティゲートウェイまたはクラスタオブジェクトにのみルールを適用することを指定します(オブジェクト名はSmartConsoleで定義されたものである必要があります)。 ■ グループオブジェクトの名前 - このグループオブジェクトのメンバであるすべてのセキュリティゲートウェイにルールを適用することを指定します(オブジェクト名はSmartConsoleで定義されているものである必要があります)。
`-n "<Rule Name>"`	オプションです。 このルールの名前(ラベル)を指定します。 **注:** ■ この文字列は二重引用符で囲む必要があります。 ■ この文字列の長さは128文字までです。 ■ この文字列の各スペースまたはバックスラッシュ文字の前に、バックスラッシュ(\)文字を記述する必要があります。例: `"This\ is\ a\ rule\ name\ with\ a\ backslash\ \\"`

パラメータ	説明
`-c "<Rule Comment>"`	オプションです。 このルールのコメントを指定します。 **注:** ■ この文字列は二重引用符で囲む必要があります。 ■ この文字列の長さは128文字までです。 ■ この文字列の各スペースまたはバックスラッシュ文字の前に、バックスラッシュ(\)文字を記述する必要があります。例: `"This\ is\ a\ comment\ with\ a\ backslash\ \\"`
`-o "<Rule Originator>"`	オプションです。 このルールの発信者名を指定します。 **注:** ■ この文字列は二重引用符で囲む必要があります。 ■ この文字列の長さは128文字までです。 ■ この文字列の各スペースまたはバックスラッシュ文字の前に、バックスラッシュ(\)文字を記述する必要があります。例: `"Created\ by\ John\ Doe"`
`-z "<Zone>"`	オプションです。 このルールのセキュリティゾーンの名前を指定します。 **注:** ■ この文字列は二重引用符で囲む必要があります。 ■ この文字列の長さは128文字までです。
`ip <IP Filter Arguments>`	必須(このipパラメータまたはquotaパラメータを使用)。 *不審なアクティビティモニタ(SAM)*ルールを設定します。 SAM規則のIP Filter Argumentsを指定します(これらのオプションのうち少なくとも1つを使用する必要があります)。 `[-C] [-s <Source IP>] [-m <Source Mask>] [-d <Destination IP>] [-M <Destination Mask>] [-p <Port>] [-r <Protocol>]` 以下の説明を参照してください。

パラメータ	説明
`quota <Quota Filter Arguments>`	必須(このquotaパラメータまたはipパラメータを使用)。 *レート制限*ルールを設定します。 レート制限ルールのQuota Filter Argumentsを指定します(以下の説明を参照)。 ■ `[flush true]` ■ `[source-negated {true | false}] source <Source>` ■ `[destination-negated {true | false}] destination <Destination>` ■ `[service-negated {true | false}] service <Protocol and Port numbers>` ■ `[<Limit1 Name> <Limit1 Value>] [<Limit2 Name> <Limit2 Value>] ...[<LimitN Name> <LimitN Value>]` ■ `[track <Track>]` **重要:** ■ Quotaルールは、セキュリティゲートウェイにすぐには適用されません。SAM(Suspicious Activity Monitoring)ポリシーデータベースへの登録のみとなります。SAMポリシーデータベースからすべてのルールをすぐに適用するには、`fw samp add`コマンド構文に"`flush true`"を追加します。 ■ 説明: 新規接続のレート(および一般的なレート制限)については、ルールの制限に違反した場合、セキュリティゲートウェイはそのルールに一致するすべてのパケットもドロップします。 セキュリティゲートウェイは、新規接続率を1秒単位で計算します。 1秒タイマーが開始されると、セキュリティゲートウェイは既存のコネクションのパケットを含むすべてのパケットを許可します。 その1秒間のある時点で、新規接続が多すぎる場合、セキュリティゲートウェイはその1秒間の残りの時間、残りのパケットをすべてブロックします。 次の1秒間のインターバルが始まると、カウンタはリセットされ、プロセスはやり直されます。セキュリティゲートウェイは、ルールの制限に違反したポイントまで、パケットの通過を再び許可します。

不審なアクティビティモニタ(SAM)ルールのIPフィルタ引数構文の説明

引数	説明
`-C`	開いている接続を閉じることを指定します。
`-s <Source IP>`	送信元IPアドレスを指定します。
`-m <Source Mask>`	送信元サブネットマスクを指定します(ドット付き10進数形式 - x.y.z.w)。
`-d <Destination IP>`	宛先IPアドレスを指定します。
`-M <Destination Mask>`	宛先サブネットマスクを指定します(ドット付き10進数形式 - x.y.z.w)。
`-p <Port>`	ポート番号を指定する(*IANA Service Name and Port Number Registry*)。
`-r <Protocol>`	プロトコル番号を指定する(*IANA Protocol Numbers*)。

レート制限ルールのクォータフィルタ引数構文の説明

引数	説明
`flush true`	クォータルールをコンパイルして、すぐにSecureXLに読み込むことを指定します。

引数	説明
`[source-negated {true | false}] source <Source>`	ソースタイプとその値を指定します。 ■ `any` このルールは、すべての送信元から送信されるパケットに適用されます。 ■ `range:<IP Address>` または `range:<IP Address Start>-<IP Address End>` このルールは次から送信されるパケットに適用されます。 • 指定されたIPv4アドレス(x.y.z.w) • 指定されたIPv6アドレス(xxxx:yyyy:....:zzz) ■ `cidr:<IP Address>/<Prefix>` このルールは次から送信されるパケットに適用されます。 • IPv4アドレス(プレフィックス:0 ~ 32) • IPv6アドレス(プレフィックス:0 ~ 128) ■ `cc:<Country Code>` このルールは、Geo IPデータベースに基づいて、この国に割り当てられたソースIPアドレスと国コードを照合します。 2文字のコードはISO 3166-1 alpha-2で定義されています。 ■ `asn:<Autonomous System Number>` このルールは、Geo IPデータベースに基づいて、この組織に割り当てられているソースIPアドレスと組織のAS番号を照合します。 有効な構文は*ASnnnn*で、*nnnn*は特定の組織に固有の番号です。 **注:** ■ デフォルト:`source-negated false` ■ `source-negated true`は、指定されたタイプを除くすべてのソースタイプを処理します。

引数	説明
`[destination-negated {true | false}] destination <Destination>`	宛先タイプとその値を指定します。 ■ `any` このルールは、すべての宛先に送信されるパケットに適用されます。 ■ `range:<IP Address>` または `range:<IP Address Start>-<IP Address End>` このルールが適用されるパケットの送信先： • 指定されたIPv4アドレス(x.y.z.w) • 指定されたIPv6アドレス(xxxx:yyyy:....:zzz) ■ `cidr:<IP Address>/<Prefix>` このルールが適用されるパケットの送信先： • IPv4アドレス(プレフィックス：0 ~ 32) • IPv6アドレス(プレフィックス：0 ~ 128) ■ `cc:<Country Code>` このルールは、Geo IPデータベースに基づいて、この国に割り当てられた宛先IPアドレスに国コードをマッチングさせます。 2文字のコードはISO 3166-1 alpha-2で定義されています。 ■ `asn:<Autonomous System Number>` このルールは、Geo IPデータベースを基に、この組織に割り当てられた宛先IPアドレスに組織のAS番号をマッチングさせます。 有効な構文は*ASnnnn*で、*nnnn*は特定の組織に固有の番号です。 **注：** ■ デフォルト：`destination-negated false` ■ `destination-negated true`は、指定されたタイプ以外のすべての宛先タイプを処理します。

引数	説明
`[service-negated {true | false}] service <Protocol and Port numbers>`	プロトコル番号を指定します (*IANA Protocol Numbers*)とポート番号 (*IANA Service Name and Port Number Registry*): ■ *<Protocol>* IPプロトコル番号 (範囲 : 1 ~ 255) ■ *<Protocol Start>-<Protocol End>* IPプロトコル番号の範囲 ■ *<Protocol>/<Port>* IPプロトコル番号 (1 ~ 255の範囲) 、TCP/UDPポート番号 (1 ~ 65535の範囲) ■ *<Protocol>/<Port Start>-<Port End>* IPプロトコル番号とTCP/UDPポート番号の範囲 (1 ~ 65535) **注 :** ■ デフォルト : `service-negated false` ■ `service-negated true`は、指定されたプロトコルとポートを持つトラフィック以外のすべてのトラフィックを処理

引数	説明
[<*Limit 1 Name*> <*Limit 1 Value*>] [<*Limit 2 Name*> <*Limit 2 Value*>] ... [<*Limit N Name*> <*Limit N Value*>]	クォータ制限とその値を指定します。 **注** - 複数のクォータ制限を設定する場合は、スペースで区切ってください。 ■ concurrent-conns <*Value*> このルールに一致する同時アクティブ接続の最大数を指定します。 ■ concurrent-conns-ratio <*Value*> セキュリティゲートウェイを介したアクティブな接続総数に対する*concurrent-conns*値の最大比率を、65536分の1の単位で指定します(計算式:N / 65536)。 ■ pkt-rate <*Value*> このルールに一致する1秒あたりの最大パケット数を指定します。 ■ pkt-rate-ratio <*Value*> セキュリティゲートウェイを経由するすべての接続のレートに対する*pkt-rate*値の最大比率を、65536分の1の単位で指定します(計算式:N / 65536)。 ■ byte-rate <*Value*> このルールに一致するパケットの1秒あたりの最大合計バイト数を指定します。 ■ byte-rate-ratio <*Value*> セキュリティゲートウェイを経由するすべての接続のバイト/秒レートに対する*バイトレート*値の最大比率を、65536分の1で指定します(計算式:N / 65536)。 ■ new-conn-rate <*Value*> ルールに一致する1秒あたりの最大接続数を指定します。 ■ new-conn-rate-ratio <*Value*> セキュリティゲートウェイを介した1秒あたりの全接続の割合に対する*new-conn-rate*値の最大割合を、65536分の1で指定する(計算式:N / 65536)。

引数	説明
[track <*Track*>]	追跡オプションを指定します。 ■ source 特定の送信元 IP アドレスの接続、パケット、バイトをカウントし、このルールの累積は行いません。 ■ source-service 特定のソースIPアドレス、特定のIPプロトコルと宛先ポートの接続、パケット、バイトをカウントし、このルールの累積は行いません。

例

例1 - 範囲によるレート制限するルール

```
fw sam_policy add -a d -l r -t 3600 quota service any source range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
```

説明:

- このルールは、既存の接続のパケットを含め、このルールで設定したクォータを超えるすべての接続(-a d)のパケットをドロップします。
- このルールで設定したクォータを超えるパケット(-l r)をログに記録します。
- このルールは3600秒後に期限切れとなります(-t 3600)。
- new-conn-rate 5このルールは、172.16.7.11 - 172.16.7.13 (source range:172.16.7.11-172.16.7.13) の範囲のソース IP アドレスからのトラフィック (service any) に対して、新しい接続の作成速度を毎秒5接続に制限します。

  注 - 1秒あたりのログエントリーの総数の制限は、*fwaccel dos config set -n <rate>*コマンドで設定します。
- このルールには"flush true"パラメータが含まれているため、SAM(Suspicious Activity Monitoring) ポリシーデータベース内の他のルールとともに、SecureXL上で直ちにコンパイルされ読み込まれます。

例2 - サービス仕様によるレート制限ルール

```
fw sam_policy add -a n -l r quota service 1,50-51,6/443,17/53 service-negated true source cc:QQ byte-rate 0
```

説明:

- このルールで設定されたクォータを超えるすべてのパケット (`-a n`) をログに記録し、通過させます。
- このルールは期限切れにならない(`timeout` パラメータが指定されていない) 。解除するには、明示的に削除する必要があります。
- `service-negated true`このルールは、IPプロトコル番号1、50～51、6ポート443、17ポート53のパケット(`service 1,50-51,6/443,17/53`)以外のすべてのパケットに適用されます。
- このルールは、指定された国コード(`cc:QQ`)を持つ国に割り当てられている送信元IPアドレスからのすべてのパケットに適用されます。
- このルールは、IPプロトコル番号1、50-51、6ポート443、17ポート53のパケット以外のトラフィックを通過させない(`byte-rate 0`)ものです。
- このルールは、「`flush true`」パラメータを含んでいないため、すぐにコンパイルされてSecureXLにインストールされるわけではありません。

例3 - ASNによるレート制限ルール

```
fw sam_policy -a d quota source asn:AS64500,cidr:[::FFFF:C0A8:1100]/120 service any pkt-rate 0
```

説明:

- このルールは、このルールに一致するすべてのパケットをドロップ(`-a d`)します。
- このルールは期限切れにならない(`timeout` パラメータが指定されていない) 。解除するには、明示的に削除する必要があります。
- このルールは、自治体番号64500(`asn:AS64500`)からのパケットに適用されます。
- このルールは、送信元 IPv6アドレス FFFF:C0A8:1100/120 (`cidr:[::FFFF:C0A8:1100]/120`) からのパケットに適用されます。
- このルールは、すべてのトラフィック(`service any`) に適用されます。
- このルールは、いかなるトラフィックも通過させません(`pkt-rate 0`)。
- このルールは、「`flush true`」パラメータを含んでいないため、すぐにコンパイルされてSecureXLにインストールされるわけではありません。

例4 - 許可リストによるレート制限ルール

```
fw sam_policy add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
```

説明:

- このルールは、このルールに一致するすべてのパケットをバイパス(`-a b`)します。

  注 - アクセスコントロールポリシーや他の種類のセキュリティポリシールールは引き続き適用されます。

- このルールは期限切れにならない(`timeout` パラメータが指定されていない)。解除するには、明示的に削除する必要があります。
- このルールは、送信元IPアドレスが172.16.8.17 - 172.16.9.121 (`range:172.16.8.17-172.16.9.121`) の範囲にあるパケットに適用されます。
- このルールは、TCPポート80(`service 6/80`)に送信されるパケットに適用されます。
- このルールは、「`flush true`」パラメータを含んでいないため、すぐにコンパイルされてSecureXLにインストールされるわけではありません。

例5 - 追跡によるレート制限ルール

```
fw sam_policy add -a d quota service any source-negated true source cc:QQ concurrent-conns-ratio 655 track source
```

説明:

- このルールは、このルールに一致するすべてのパケットをドロップ(`-a d`)します。
- このルールはパケットを記録しません(`-l r` パラメータは指定されません)。
- このルールは期限切れにならない(`timeout` パラメータが指定されていない)。解除するには、明示的に削除する必要があります。
- このルールは、すべてのトラフィック(`service any`) に適用されます。
- このルールは、指定された国コードの国に割り当てられたソースIPアドレス(`source-negated true`)を除くすべてのソースに適用されます(`cc:QQ`)。
- このルールは、指定された国コード(`concurrent-conns-ratio 655`)を持つ国に割り当てられているソースIPアドレスからの接続(`service any`)を除くすべてのトラフィック(`service-negated true`)に対して、同時アクティブ接続の最大数を655/65536=~1%(`cc:QQ`)に制限します。
- このルールは、一致するソースからのトラフィックのみの接続、パケット、およびバイトをカウントし、このルールの累積ではありません。
- このルールは、「`flush true`」パラメータを含んでいないため、すぐにコンパイルされてSecureXLにインストールされるわけではありません。

fw sam_policy batch

説明

"`fw sam_policy batch`"と"`fw6 sam_policy batch`"コマンド:

- 一度に多くのSAM(Suspicious Activity Monitoring) ルールを追加/削除することができます。
- 一度に多くのレート制限ルールを追加/削除することができます。

注:

- これらのコマンドは互換性があります。
  - IPv4の場合: "`fw sam_policy`"および"`fw samp`"
  - IPv6の場合: "`fw6 sam_policy`"および"`fw6 samp`"
- Gaia Clishまたはエキスパートモードでこれらのコマンドのいずれかを実行します。
- セキュリティゲートウェイは、SAM Policyのルールを`$FWDIR/database/sam_policy.db`ファイルに保存します。
- Security Gartner Magic Quadrant は、SAM ポリシー管理設定を`$FWDIR/database/sam_policy.mng` ファイルに保存します。

重要:

- これらのコマンドで設定した内容は、再起動後も有効になります。
- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- クラスタでは、すべてのクラスタメンバを同じ方法で設定する必要があります。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。
- VSNextモードと従来のVSXモードは、SAM(Suspicious Activity Monitoring) ルールをサポート**しません**。sk79700を参照してください。

ベストプラクティスSAMポリシーのルールは、セキュリティゲートウェイのCPUリソースを消費します。ルールの有効期限は、調査するための時間を確保しつつ、パフォーマンスに影響を与えないように設定します。必要なSAMポリシールールだけを残しておきます。リスクがあるアクティビティを確認した場合、セキュリティポリシーの編集、ユーザへの教育など、リスクへの対応を行います。

手順

1. **バッチモードの開始**

   - IPv4の場合は、次を実行します。

     ```
     fw sam_policy batch << EOF
     ```

   - IPv6の場合は、次を実行します。

     ```
     fw6 sam_policy batch << EOF
     ```

2. **該当するコマンドを入力**

   - 各行に"add"または"del"コマンドを1つずつ、必要な数だけ入力します。

     各行の先頭は、"add"または"del"パラメータのみです ("fw samp"は不可)。

   - これらのコマンドで説明されているのと同じパラメータと値のセットを使用します。

     - *fw sam_policy add (897ページ)*
     - *fw sam_policy del (913ページ)*

   - 各行をリターン(ASCII 10 - ラインフィード) 文字で終了させます(Enterキーを押す) 。

3. **バッチモードの終了**

   EOF と入力し、Enterキーを押します。

IPv4のレート制限ルールの例

```
[Expert@HostName]# fw samp batch <<EOF

add -a d -l r -t 3600 -c "Limit\ conn\ rate\ to\ 5\ conn/sec from\ these\ sources" quota
service any source range:172.16.7.13-172.16.7.13 new-conn-rate 5

del <501f6ef0,00000000,cb38a8c0,0a0afffe>

add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80

EOF
[Expert@HostName]#
```

fw sam_policy del

説明

"fw sam_policy del"と"fw6 sam_policy del"コマンド:

- 設定したSuspicious Activity Monitoring(SAM) ルールを一度に1つ削除します。
- 設定されたレート制限ルールを1つずつ削除します。

注:

- これらのコマンドは互換性があります。
  - IPv4の場合: "fw sam_policy"および"fw samp"
  - IPv6の場合: "fw6 sam_policy"および"fw6 samp"
- Gaia Clishまたはエキスパートモードでこれらのコマンドのいずれかを実行します。
- セキュリティゲートウェイは、SAM Policyのルールを$FWDIR/database/sam_policy.dbファイルに保存します。
- Security Gartner Magic Quadrant は、SAM ポリシー管理設定を $FWDIR/database/sam_policy.mng ファイルに保存します。

重要:

- これらのコマンドで設定した内容は、再起動後も有効になります。
- このコマンドはエキスパートモードまたはGaia Clish(Scalable Platform上のGaia gClish) で実行できます。
- クラスタでは、すべてのクラスタメンバを同じ方法で設定する必要があります。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。
- VSNextモードと従来のVSXモードは、SAM(Suspicious Activity Monitoring) ルールをサポート**しません**。sk79700を参照してください。

ベストプラクティスSAMポリシーのルールは、セキュリティゲートウェイのCPUリソースを消費します。ルールの有効期限は、調査するための時間を確保しつつ、パフォーマンスに影響を与えないように設定します。必要なSAMポリシールールだけを残しておきます。リスクがあるアクティビティを確認した場合、セキュリティポリシーの編集、ユーザへの教育など、リスクへの対応を行います。

IPv4の構文

```
fw [-d] sam_policy del '<Rule UID>'
```

IPv6の構文

```
fw6 [-d] sam_policy del '<Rule UID>'
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`'<Rule UID>'`	削除したいルールのUIDを指定します。 **重要:** ■ 引用符と角括弧(`'<...>'`)は必須です。 ■ ルールのUIDを確認するには*fw sam_policy get (916ページ)*コマンドを実行します。

手順

1. **不審なアクティビティモニタリング ポリシーデータベースのすべての既存のルールをリスト**

   Suspicious Activity Monitoring ポリシー データベースにある既存のルールをすべてリストします。

   ■ IPv4の場合は、次を実行します。

   ```
   fw sam_policy get
   ```

   ■ IPv6の場合は、次を実行します。

   ```
   fw6 sam_policy get
   ```

   ルールはこのような形式で表示されます。

   ```
   operation=add uid=<Value1,Value2,Value3,Value4> target=...
   timeout=... action=... log= ... name= ... comment=...
   originator= ... src_ip_addr=... req_tpe=...
   ```

   IPv4の例:

   ```
   operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a>
   target=all timeout=300 action=notify log=log name=Test\ Rule
   comment=Notify\ about\ traffic\ from\ 1.1.1.1
   originator=John\ Doe src_ip_addr=1.1.1.1 req_tpe=ip
   ```

2. **リストからUIDでルールを削除**

   - IPv4の場合は、次を実行します。

     ```
     fw [-d] sam_policy del '<Rule UID>'
     ```

   - IPv6の場合は、次を実行します。

     ```
     fw6 [-d] sam_policy del '<Rule UID>'
     ```

   IPv4の例：

   ```
   fw samp del '<5ac3965f,00000000,3403a8c0,0000264a>'
   ```

3. **フラッシュ専用ルールの追加**

   - IPv4の場合は、次を実行します。

     ```
     fw samp add -t 2 quota flush true
     ```

   - IPv6の場合は、次を実行します。

     ```
     fw6 samp add -t 2 quota flush true
     ```

   説明：

   `fw samp del`"と"`fw6 samp del`"コマンドは、永続データベースからルールを削除するだけです。セキュリティゲートウェイは、次にポリシーをコンパイルして読み込むまで、削除されたルールを適用し続けます。ルールを直ちに強制的に削除するには、"`fw samp del`"と"`fw6 samp del`"コマンドの直後にフラッシュ専用ルールを入力する必要があります。このフラッシュ専用ルールは、前のステップで指定したルールを直ちに削除し、2秒後にタイムアウトします。

   ベストプラクティス - フラッシュ専用ルールに短いタイムアウト時間を指定します。これにより、データベース内に古くなったルールが蓄積されるのを防ぐことができます。

fw sam_policy get

説明

"fw sam_policy get"と"fw6 sam_policy get"コマンド:

- 設定されているすべてのSuspicious Activity Monitoring (SAM) ルールを表示します。
- 設定されているすべてのレート制限ルールを表示します。

注:

- これらのコマンドは互換性があります。
  - IPv4の場合: "fw sam_policy"および"fw samp"
  - IPv6の場合: "fw6 sam_policy"および"fw6 samp"
- Gaia Clishまたはエキスパートモードでこれらのコマンドのいずれかを実行します。
- セキュリティゲートウェイは、SAM Policyのルールを$FWDIR/database/sam_policy.dbファイルに保存します。
- Security Gartner Magic Quadrant は、SAM ポリシー管理設定を $FWDIR/database/sam_policy.mng ファイルに保存します。

重要:

- これらのコマンドで設定した内容は、再起動後も有効になります。
- このコマンドはエキスパートモードまたはGaia Clish(Gaia gClish on Scalable Platform) で実行できます。
- クラスタでは、すべてのクラスタメンバを同じ方法で設定する必要があります。
- スケーラブルプラットフォーム(ElasticXL、Maestro、シャーシ) では、該当するセキュリティグループのGaia Portalに接続する必要があります。
- VSNextモードと従来のVSXモードは、SAM(Suspicious Activity Monitoring) ルールをサポート**しません**。sk79700を参照してください。

ベストプラクティスSAMポリシーのルールは、セキュリティゲートウェイのCPUリソースを消費します。ルールの有効期限は、調査するための時間を確保しつつ、パフォーマンスに影響を与えないように設定します。必要なSAMポリシールールだけを残しておきます。リスクがあるアクティビティを確認した場合、セキュリティポリシーの編集、ユーザへの教育など、リスクへの対応を行います。

IPv4の構文

```
fw [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

IPv6の構文

```
fw6 [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

パラメータ

注 - これらのパラメータはすべてオプションです。

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-l`	ルールの出力方法を制御します。 ■ デフォルトの形式 ("`-l`"なし) では、各ルールが別の行に出力されます。 ■ リスト形式 ("`-l`"付き) では、ルールの各パラメータを1行に区切って出力します。 ■ 参照: *fw sam_policy add (897ページ)*。
`-u '<Rule UID>'`	Rule UIDまたはゼロベースのルールインデックスで指定されたルールを表示します。 引用符と角括弧 ('<...>') は必須です。
`-k '<Key>'`	指定した述語キーを持つルールを出力します。 引用符は必須です。
`-t <Type>`	指定した述語の型を持つルールを出力します。 レート制限ルールでは、常に「`-t in`」を使用する必要があります。
`+{-v '<Value>'}`	指定した述語の値を持つルールを出力します。 引用符は必須です。
`-n`	これらの述語パラメータで指定された条件を取り消します。 ■ `-k` ■ `-t` ■ `+-v`

例

例 1 - デフォルトフォーマットでの出力

```
[Expert@HostName:0]# fw samp get

operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

例2 - リスト形式での出力

```
[Expert@HostName:0]# fw samp get -l

uid
<5ac3965f,00000000,3403a8c0,0000264a>
target
all
timeout
2147483647
action
notify
log
log
name
Test\ Rule
comment
Notify\ about\ traffic\ from\ 1.1.1.1
originator
John\ Doe
src_ip_addr
1.1.1.1
req_type
ip
```

例3 - ルールUIDでルールを出力

```
[Expert@HostName:0]# fw samp get -u '<5ac3965f,00000000,3403a8c0,0000264a>'
0
operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

例4 - 指定されたフィルタに一致するルールを出力

```
[Expert@HostName:0]# fw samp get
no corresponding SAM policy requests
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d -l r -t 3600 quota service any source
range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a n -l r quota service 1,50-51,6/443,17/53 service-negated
true source cc:QQ byte-rate 0
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a b quota source range:172.16.8.17-172.16.9.121 service
6/80
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d quota service any source-negated true source cc:QQ
concurrent-conns-ratio 655 track source
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3586 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service' -t in -v '6/80'
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service-negated' -t in -v 'true'
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source' -t in -v 'cc:QQ'
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k source -t in -v 'cc:QQ' -n
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3291 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source-negated' -t in -v 'true'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'byte-rate' -t in -v '0'
operation=add uid=<5baa9431,00000000,860318ac,00002efd> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'flush' -t in -v 'true'
operation=add uid=<5baa9422,00000000,860318ac,00002eea> target=all timeout=2841 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'concurrent-conns-ratio' -t in -v '655'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
```

```
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
```

fwm

説明

さまざまな管理業務を行い、管理情報を表示します。

注:

- デバッグ方法については、`fwm`のsk97638プロセスの説明を参照してください。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこれらのコマンドを実行する必要があります。

構文

```
fwm [-d]
       dbload <options>
       exportcert <options>
       fetchfile <options>
       fingerprint <options>
       getpcap <options>
       ikecrypt <options>
       load [<options>]
       logexport <options>
       mds <options>
       printcert <options>
       sic_reset
       snmp_trap <options>
       unload [<options>]
       ver [<options>]
       verify <options>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。

パラメータ	説明
`dbload <options>`	ユーザデータベースとネットワークオブジェクト情報を指定したターゲットにダウンロードします。 参照: *fwm dbload (925ページ)*。
`exportcert <options>`	指定されたオブジェクトのSIC証明書をファイルにエクスポートします。 参照: *fwm exportcert (926ページ)*。
`fetchfile <options>`	指定されたソースコンピュータから指定されたOPSEC設定ファイルを取得します。 参照: *fwm fetchfile (927ページ)*。
`fingerprint <options>`	Check Pointのフィンガープリントを表示します。 参照: *fwm fingerprint (928ページ)*。
`getpcap <options>`	指定したSecurity GatewayからIPSのパケットキャプチャデータを取得します。 参照: *fwm getpcap (930ページ)*。
`ikecrypt <options>`	秘密キーで暗号化します。 参照: *fwm ikecrypt (932ページ)*。
`load <options>`	このコマンドは、R80以降では廃止されています。 *mgmt_cli (978ページ)*コマンドを使用して、マネージドセキュリティゲートウェイにポリシーを読み込みます。 参照: *fwm load (933ページ)*。
`logexport <options>`	セキュリティログファイル(`$FWDIR/log/*.log`)または監査ログファイル(`$FWDIR/log/*.adtlog`)をASCIIファイルにエクスポートします。 参照: *fwm logexport (934ページ)*。
`mds <options>`	マルチドメインサーバの情報を表示し、各種操作を実行できます。 参照: *fwm mds (939ページ)*。
`printcert <options>`	SIC証明書の詳細が表示されます。 参照: *fwm printcert (941ページ)*。
`sic_reset`	管理サーバのSICをリセットします。 参照: *fwm sic_reset (947ページ)*。
`snmp_trap <options>`	指定ホストにSNMP Trapを送信します。 参照: *fwm snmp_trap (948ページ)*。
`unload <options>`	指定された管理対象のSecurity Gatewayからポリシーをアンロードします。 参照: *fwm unload (951ページ)*。

パラメータ	説明
`ver <options>`	管理サーバのCheck Pointバージョンを表示します。 参照: *fwm ver (955ページ)*。
`verify <options>`	このコマンドは、R80以降では廃止されています。 *mgmt_cli (978ページ)*コマンドを使用してポリシーを検証します。 参照: *fwm verify (956ページ)*。

fwm dbload

説明

ユーザデータベースとネットワークオブジェクト情報を、1つ以上の**Management** Software Bladesが有効になっている指定された管理対象サーバにコピーします。

重要 - このコマンドは、R80以降では使われていません。
API コマンド "`install-database`" を使用して、該当するサーバにデータベースをインストールします。
詳細は*Check Point Management API Reference*。

fwm exportcert

説明

指定された管理対象オブジェクトのSIC証明書をファイルにエクスポートします。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] exportcert -obj <Name of Object> -cert <Name of CA> -file
<Output File> [-withroot] [-pem]
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、fwmのsk97638プロセスの説明を参照してください。
<Name of Object>	証明書をエクスポートする管理対象オブジェクトの名前を指定します。
<Name of CA>	エクスポートする証明書の認証局名を指定します。
<Output File>	出力ファイル名を指定します。
-withroot	証明書の内容に加え、証明書のルートもエクスポートします。
-pem	エクスポートした情報をテキストファイルで保存します。 デフォルトでは、バイナリファイルに保存されます。

fwm fetchfile

説明

指定されたソースコンピュータから指定されたOPSEC設定ファイルを取得します。

このコマンドは、`fwopsec.conf`または`fwopsec.v4x`のファイルのみをサポートします。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] fetchfile -r <File> [-d <Local Path>] <Source>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-r <File>`	相対的な`fw1`ディレクトリを指定します。 このコマンドは、これらのファイルのみに対応しています。 ■ `conf/fwopsec.conf` ■ `conf/fwopsec.v4x`
`-d <Local Path>`	取得したファイルを保存するローカルディレクトリを指定します。
<Source>	ファイルの取得元である管理対象のリモートコンピュータを指定します。 **注** - ローカルとリモートのソースコンピュータは、SICの信頼関係を確立している必要があります。

例

```
[Expert@MGMT:0]# fwm fetchfile -r "conf/fwopsec.conf" -d /tmp 192.168.3.52
Fetching conf/fwopsec.conf from 192.168.3.52...
Done
[Expert@MGMT:0]#
```

fwm fingerprint

説明

Check Pointのフィンガープリントを表示します。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] fingerprint [-d]
      <IP address of Target> <SSL Port>
      localhost <SSL Port>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 デバッグオプション: ■ `fwm -d` すべての`fwm`アクションの完全デバッグを実行します。 完全なデバッグ手順については、`fwm` のsk97638 プロセスの説明を参照してください。 ■ `fingerprint -d` フィンガープリントアクションに対してのみデバッグを実行します。
<IP address of Target>	リモート管理コンピュータのIPアドレスを指定します。
<SSL Port>	SSLポート番号を指定します。 デフォルトは443です。

例 1 - ローカル管理サーバのフィンガープリントを表示する場合

```
[Expert@MGMT:0]# fwm fingerprint localhost 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email
Address,CN=192.168.3.51,L=Locality Name (eg\, city)
#FINGER 11:A6:F7:1F:B9:F5:15:BC:F9:7B:5F:DC:28:FC:33:C5
##
[Expert@MGMT:0]#
```

例 2 - マネージドセキュリティゲートウェイからのフィンガープリントを表示する場合

```
[Expert@MGMT:0]# fwm fingerprint 192.168.3.52 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email
Address,CN=192.168.3.52,L=Locality Name (eg\, city)
#FINGER 5C:8E:4D:B9:B4:3A:58:F3:79:18:F1:70:99:8B:5F:2B
##
[Expert@MGMT:0]#
```

fwm getpcap

説明

指定したSecurity GatewayからIPSのパケットキャプチャデータを取得します。

このコマンドは、Security Gatewayの`$FWDIR/log/captures_repository/`ディレクトリに保存されているIPSパケットキャプチャに対してのみ機能します。

このコマンドは、Security Gatewayの`$FWDIR/log/blob/`ディレクトリにパケットキャプチャを保存するAnti-BotやAnti-Virusなどの他のSoftware Bladeでは機能しません。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] getpcap -g <Security Gateway> -u '{<Capture UID>}' -p
<Local Path>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、`fwm`のsk97638プロセスの説明を参照してください。
`-g <Security Gateway>`	SmartConsoleで設定されているSecurity Gatewayオブジェクトのメインアドレスまたは名前を指定します。
`-u '{<Capture UID>}'`	パケットキャプチャファイルのUnique IDを指定します。 パケットキャプチャファイルのユニークIDを確認するには、該当するログファイルを**SmartConsole > Logs & Events > Logs**で開いてください。
`-p <Local Path>`	指定されたパケットキャプチャファイルを保存するローカルパスを指定します。 ローカルディレクトリを明示的に指定しない場合、パケットキャプチャファイルは現在の作業ディレクトリに保存されます。

例

```
[Expert@MGMT:0]# fwm getpcap -g 192.168.162.1 -u '{0x4d79dc02,0x10000,0x220da8c0,0x1ffff}'
/var/log/
[Expert@MGMT:0]#
```

fwm ikecrypt

説明

IKEを使用してEndpoint VPN Clientユーザのパスワードを暗号化します。その結果得られた文字列をLDAPデータベースに格納する必要があります。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] ikecrypt <Key> <Password>
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、script コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、fwmのsk97638 プロセスの説明を参照してください。
<Key>	LDAP Account Unitプロパティウィンドウの**Encryption**タブで定義されているIKEキーを指定します。
<Password>	Endpoint VPN クライアントユーザのパスワードを指定します。

例

```
[Expert@MGMT:0]# fwm ikecrypt MySecretKey MyPassword
OUQJHiNHCj6HJGH8ntnKQ7tg
[Expert@MGMT:0]#
```

fwm load

説明

マネージドセキュリティゲートウェイにポリシーを読み込みます。

重要 - このコマンドは、R80以降では使われていません。
管理対象のセキュリティゲートウェイにポリシーをロードするには、API コマンド "`install-policy`" を使用します。
詳細は*Check Point Management API Reference*。

fwm logexport

説明

セキュリティログファイル(`$FWDIR/log/*.log`)または監査ログファイル(`$FWDIR/log/*.adtlog`)をASCIIファイルにエクスポートします。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm logexport -h
```

```
fwm [-d] logexport [{-d <Delimiter> | -s}] [-t <Table Delimiter>] [-i <Input File>] [-o <Output File>] [{-f | -e}] [-x <Start Entry Number>] [-y <End Entry Number>] [-z] [-n] [-p] [-a] [-u <Unification Scheme File>] [-m {initial | semi | raw}]
```

パラメータ

パラメータ	説明
`-h`	ビルトインの使用状況を表示します。
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、`fwm`のsk97638プロセスの説明を参照してください。
`-d <Delimiter> | -s`	ログエントリのフィールド間の出力区切り文字を指定します。 ■ `-d <Delimiter>`- 指定された区切り文字を使用。 ■ `-s`- 区切り文字としてASCII文字#255(改行しないスペース)を使用。 **注** - 区切り文字を明示的に指定しない場合、デフォルトはセミコロン(;)です。

パラメータ	説明
`-t <Table Delimiter>`	テーブルフィールド内の出力区切り文字を指定します。 テーブルフィールドは、次のようになります。 *ROWx:COL0,ROWx:COL1,ROWx:COL2*など。 **注** - 表の区切り文字を明示的に指定しない場合、デフォルトはコンマ(,)です。
`-i <Input File>`	入力ログファイル名を指定します。 **注:** ■ このコマンドは、セキュリティログファイル(`$FWDIR/log/*.log`)と監査ログファイル(`$FWDIR/log/*.adtlog`)のみをサポートします。 ■ 入力ログファイルを明示的に指定しない場合、コマンドはアクティブなセキュリティログファイル`$FWDIR/log/fw.log`
`-o <Output File>`	出力ファイル名を指定します。 **注** - 出力ログファイルを明示的に指定しない場合、コマンドはその出力を画面に表示します。
`-f`	現在開いているログファイルの最後に達した後、ログファイルを無期限に監視し続け、新しいエントリもエクスポートするように指定します。 **注** - *アクティブな*ログファイルのみに適用:`$FWDIR/log/fw.log`または`$FWDIR/log/fw.adtlog`
`-e`	現在開いているログファイルの最後に達した後、ログファイルを無期限に監視し続け、新しいエントリも同様にエクスポートします。 **注** - *アクティブな*ログファイルのみに適用:`$FWDIR/log/fw.log`または`$FWDIR/log/fw.adtlog`
`-x <Start Entry Number>`	指定した番号以下のログエントリを、ログファイルの先頭から数えてエクスポートを開始します。
`-y <End Entry Number>`	ログファイルの先頭から数えて、指定された番号までのログエントリのエクスポートを開始します。
`-z`	エラー(間違ったフィールド値など)の場合、ログエントリのエクスポートを継続するように指定します。 デフォルトの動作は停止です。
`-n`	ログファイルに含まれるIPアドレスのDNS解決を行わないことを指定します(デフォルトの動作)。 これにより、ログの処理が大幅に高速化されます。

パラメータ	説明
`-p`	ログファイル中のポート番号の解決を行わないように指定します(デフォルトの動作) 。 これにより、ログの処理が大幅に高速化されます。
`-a`	アカウントログエントリのみをエクスポートします。
`-u <Unification Scheme File>`	ログ統一スキームファイルのパスと名前を指定します。 デフォルトのログ統一スキームファイル: `$FWDIR/conf/log_unification_scheme.C`
`-m {initial | semi | raw}`	ログ統一モードを指定します。 ■ `initial`- ログエントリの完全な統一。このコマンドは、各IDに対して1つのユニファイドログエントリをエクスポートします。これはデフォルトです。 "`-f`"パラメータも指定した場合、更新は一切出力されず、新規接続の開始に関連するエントリのみが出力されます。アップデートもエクスポートするには、"`semi`"パラメータを使用します。 ■ `semi`- ログエントリを段階的に統一。各ログエントリについて、以前に同じIDを持つエントリがあった場合は、すべてこのエントリと統合するエクスポートエントリ。 ■ `raw`- ログを統一しない。すべてのログエントリをエクスポートします。

`fwm logexport`コマンドの出力は、表形式で表示されます。

最初の行は、ログエントリに含まれるすべてのログフィールドの名前をリストアップします。

次の行は、それぞれ1つのログエントリからなり、そのフィールドは最初の行と同じ順序でソートされています。

ログエントリに特定のフィールドの情報がない場合、このフィールドは空のままです(2つの連続したセミコロン";;"で示されます)。

コマンドの出力に表示されるログのフィールドを制御することができます。

ステップ	手順
1	`$FWDIR/conf/logexport.ini`ファイルを作成します。 `[Expert@MGMT:0]# touch $FWDIR/conf/logexport.ini`
2	`$FWDIR/conf/logexport.ini`ファイルを編集します。 `[Expert@MGMT:0]# vi $FWDIR/conf/logexport.ini`

3	ログフィールドを出力に含めたり除外したりするには、設定ファイルに以下の行を追加してください。
	`[Fields_Info]`
	`included_fields = field1,field2,field3,<REST_OF_FIELDS>,field100`
	`excluded_fields = field10,field11`
	各変数の意味は以下のとおりです。
	■ `included_fields`パラメータのみ、`excluded_fields`パラメータのみ、または両方を指定することができます。
	■ `num`フィールドは常に最初に表示されます。このフィールドを操作することはできません。
	■ `<REST_OF_FIELDS>`は、フィールドのリストを参照するオプションの予約済みトークンです。
	• "`-f`"パラメータを指定した場合、`<REST_OF_FIELDS>`は`$FWDIR/conf/logexport_default.C`ファイルのフィールドのリストに基づいています。
	• "`-f`"パラメータを指定しない場合、`<REST_OF_FIELDS>`は入力ログファイルに基づいています。

4	変更をファイルに保存し、Viエディタを終了します。
5	ログをエクスポートします。 `fwm logexport <options>`

例 1 - すべてのログエントリをエクスポートする場合

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_
rule_name;fg-1_client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
0;13Jun2018;19:47:54;CXL1_192.168.3.52;control; ;;daemon;inbound;VPN-1 & FireWall-1;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_Server.checkpoint.com.s6t98x;5;18446744073709551615;2;Log
file has been switched to: MyLog.log;Network;;;;;;;;;;;;
1;13Jun2018;19:47:54;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;;;;;;;;;;
... ...
35;13Jun2018;19:55:59;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host
Redirect;;;;;;;;;
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>
;1;;;
... ...
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Coul
d not reach "https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and
Proxy configuration on the gateway.;2;Contracts may be out-of-date
... ...
[Expert@MGMT:0]#
```

例2 - 指定した番号のログエントリのみをエクスポートする場合

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log -x 36 -y 47
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_
rule_name;fg-1_client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>
;1;;;
37;13Jun2018;19:56:06;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;2;;Network;Default;Default;Host
Redirect;;;;;;;;;
... ...
46;13Jun2018;19:56:59;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host
Redirect;;;;;;;;;
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Coul
d not reach "https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and
Proxy configuration on the gateway.;2;Contracts may be out-of-date
[Expert@MGMT:0]#
```

fwm mds

説明

- マルチドメインサーバのCheck Pointのバージョンを表示します。
- Global VPN Communitiesのステータスツリーを再構築します。

注 - マルチドメインサーバでは、このコマンドを実行することができます。

- MDSのコンテキストで

```
mdsenv
```

- ドメイン管理サーバのコンテキストで

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] mds
      ver
      rebuild_global_communities_status {all | missing}
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、`fwm`のsk97638プロセスの説明を参照してください。
`ver`	マルチドメインサーバのCheck Pointのバージョンを表示します。
`rebuild_global_communities_status`	Global VPN Communitiesのステータスツリーを再構築します。 - `all`- すべてのグローバルVPNコミュニティのステータスツリーを再構築します。 - `missing`- ステータスツリーを持たないグローバルVPNコミュニティに対してのみ、ステータスツリーを再構築します。

例

```
[Expert@MDS:0]# fwm mds ver
This is Check Point Multi-Domain Security Management R82 - Build
11
[Expert@MDS:0]#
```

fwm printcert

説明

SIC証明書の詳細が表示されます。

注:
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] printcert
      -obj <Name of Object> [-cert <Certificate Nick Name>] [-
verbose]
      -ca <CA Name> [-x509 <Name of File> [-p]] [-verbose]
      -f <Name of Binary Certificate File> [-verbose]
```

パラメータ

項目	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、`fwm`のsk97638プロセスの説明を参照してください。
`-obj <Name of Object>`	SIC証明書情報を表示する管理対象オブジェクトの名前を指定します。
`-cert <Certificate Nick Name>`	証明書のニックネームを指定します。
`-ca <CA Name>`	認証局名を指定します。 **注** - Check Point CA名は`internal_ca`です。
`-x509 <Name of File>`	X.509ファイルの名前を指定します。
`-p`	SIC証明書をテキストファイルで表示することを指定します。
`-f <Name of Binary Certificate File>`	表示するバイナリSIC証明書ファイルを指定します。
`-verbose`	冗長モードで情報を表示します。

例

例1 - 管理サーバのSIC証明書の表示

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca
Subject: O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Apr 8 13:41:00 2018 Local Time
Not Valid After: Fri Jan 1 05:14:07 2038 Local Time
Serial No.: 1
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Key Usage:
        digitalSignature
        keyCertSign
        cRLSign
Basic Constraint:
        is CA
MD5 Fingerprint:
   7B:F9:7B:4C:BD:40:B9:1C:AB:2C:AE:CF:66:2E:E7:06
SHA-1 Fingerprints:
1. A6:43:3A:2B:1A:04:7F:A6:36:A6:2C:78:BF:22:D9:BC:F7:7E:4D:73
2. KEYS HEM GERM PIT ABUT ROVE RAW PA IQ FAWN NUT SLAM
[Expert@MGMT:0]#
```

例2 - 管理サーバのSIC証明書を冗長モードで表示

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca -verbose
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: called
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: closing existing database
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] do_links_getver: strncmp failed. Returning -2
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] db_fetchkey: entering
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] PubKey:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Modulus:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ae b3 75 36 64 e4 1a 40 fe c2 ad 2f 9b 83 0b 45
f1 00 04 bc
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 77 77 76 d1 de 8a cf 9f 32 78 8b d4 b1 b4 be
db 75 cc c8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c2 6d ff 3e aa fe f1 2b c3 0a b0 a2 a5 e0 a8 ab
45 cd 87 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ac c6 9f a4 a9 ba 30 79 08 fa 59 4c d2 dc 3d 36
ca 17 d7 c1
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] b2 a2 41 f5 89 0f 00 d4 2d f2 55 d2 30 a5 32 c7
46 7a 6b 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 29 0f 53 9f 35 42 91 e5 7d f7 30 6d bc b3 f2 ae
f3 f0 ed 88
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c4 d7 7d 0c 2d f6 5f c8 ed 9f 9a 57 54 79 d0 0f
0b 2f 9c 0d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 94 2e f0 f4 66 62 f7 ae 2e f8 8e 90 08 ba 63 85
b6 46 2f b7
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a7 01 29 9a 14 58 a8 ef eb 07 17 4e 95 8b 2f 48
5f d3 18 10
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 00 d5 03 d7 fd 45 45 ca 67 5b 34 be b8 00 ae
ea 9a cd 50
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] d6 e7 a2 81 86 78 11 d7 bf 04 9f 8b 43 3f f7 36
5f ed 31 a8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a3 9d 8b 0a de 05 fb 5c 44 2e 29 e3 3e f4 dd 50
01 0f 86 9d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 55 16 a3 4d f8 90 2d 13 c6 c1 28 57 f8 3e 7c 59
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Exponent: 65537 (0x10001)
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52]
X509 Certificate Version 3
refCount: 1
Serial Number: 1
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Apr 8 13:41:00 2018 Local Time
Not valid after: Fri Jan 1 05:14:07 2038 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyCertSign
                cRLSign
        Basic Constraint (Critical):
                is CA

[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] destroy_rand_mutex: destroy
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] cpKeyTaskManager::~cpKeyTaskManager: called.
[Expert@MGMT:0]#
```

例3 - 管理クラスタオブジェクトのSIC証明書の表示

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244

printing all certificates of CXL_192.168.3.244

defaultCert:
Host Certificate (level 0):
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Jun 3 19:58:19 2018 Local Time
Not Valid After: Sat Jun 3 19:58:19 2023 Local Time
Serial No.: 85021
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Subject Alternate Names:
        IP Address: 192.168.3.244
CRL distribution points:
        http://192.168.3.240:18264/ICA_CRL2.crl
        CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x
Key Usage:
        digitalSignature
        keyEncipherment
Basic Constraint:
        not CA
MD5 Fingerprint:
   B1:15:C7:A8:2A:EE:D1:75:92:9F:C7:B4:B9:BE:42:1B
SHA-1 Fingerprints:
1. BC:7A:D9:E2:CD:29:D1:9E:F0:39:5A:CD:7E:A9:0B:F9:6A:A7:2B:85
2. MIRE SANK DUSK HOOD HURD RIDE TROY QUAD LOVE WOOD GRIT WITH


               *****
[Expert@MGMT:0]#
```

例4 - 管理クラスタオブジェクトのSIC証明書を冗長モードで表示

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244 -verbose
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: called
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: closing existing database
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] do_links_getver: strncmp failed. Returning -2

printing all certificates of CXL_192.168.3.244

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] db_fetchkey: entering
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 1 certificates
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] PubKey:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Modulus:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] df 35 c3 45 ca 42 16 6e 21 9e 31 af c1 fd 20 0a
3d 5b 6f 5d
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] e0 a2 0c 0e fa fa 5e e5 91 9d 4e 73 77 fa db 86
0b 5e 5d 0c
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] ce af 4a a4 7b 30 ed b0 43 7d d8 93 c5 4b 01 f4
3d b5 d8 f4
... ... ...
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 34 b1 db ac 18 4f 11 bd d2 fb 26 7d 23 74 5c d9
00 a1 58 1e
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 60 7c 83 44 fa 1e 1e 86 fa ad 98 f7 df 24 4a 21
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Exponent: 65537 (0x10001)
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45]
X509 Certificate Version 3
refCount: 1
Serial Number: 85021
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Jun 3 19:58:19 2018 Local Time
Not valid after: Sat Jun 3 19:58:19 2023 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyEncipherment
        Subject Alternate names:
                IP: 192.168.3.244
        Basic Constraint:
                not CA
        CRL distribution Points:
                URI: http://192.168.3.240:18264/ICA_CRL2.crl
                DN: CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x

defaultCert:

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] destroy_rand_mutex: destroy
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] cpKeyTaskManager::~cpKeyTaskManager: called.
                *****
[Expert@MGMT:0]#
```

fwm sic_reset

説明

管理サーバのSICをリセットします。

詳細な手順については、sk65764: How to reset SICを参照してください。

警告:

- **このコマンドを実行する前に、管理サーバのGaiaスナップショットとフルバックアップを取ってください。**
  このコマンドは、管理サーバとそのすべての管理オブジェクト間のSICをリセットします。
- **この操作により、管理される環境全体にわたり、すべての内部CA証明書とSICの信頼が失われます。**
  そのため、実際の災害時リカバリを除いては、お勧めしません。

注意
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] sic_reset
```

パラメータ

パラメータ	説明
-d	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、scriptコマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、fwmのsk97638プロセスの説明を参照してください。

fwm snmp_trap

説明

指定ホストにSNMPv1 Trapを送信します。

注:

- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- Multi-Domain Serverでは、SNMP Trapパケットはリーディングインタフェースの IPアドレスから送信されます。

構文

```
fwm [-d] snmp_trap [-v <SNMP OID>] [-g <Generic Trap Number>] [-s
<Specific Trap Number>] [-p <Source Port>] [-c <SNMP Community>]
<Target> ["<Message>"]
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、`fwm`のsk97638プロセスの説明を参照してください。
`-v <SNMP OID>`	メッセージとバインドするSNMP OID(オプション)を指定します。
`-g <Generic Trap Number>`	汎用トラップ番号を指定します。 次のうち1つの値になります。 ■ 0 - `coldStart`トラップ ■ 1 - `warmStart`トラップ ■ 2 - `linkDown`トラップ ■ 3 - `linkUp`トラップ ■ 4 - `authenticationFailure`トラップ ■ 5 - `egpNeighborLoss`トラップ ■ 6 - `enterpriseSpecific`トラップ(デフォルト値)
`-s <Specific Trap Number>`	固有のトラップタイプを指定します。 汎用トラップ値が6(`enterpriseSpecific`)の場合のみ有効です。 デフォルト値は0です。
`-p <Source Port>`	SNMP Trapパケットの送信元ポートを指定します。
`-c <SNMP Community>`	SNMPコミュニティを指定します。
`<Target>`	SNMP Trapパケットの送信先となる管理対象ホストを指定します。 解決可能なホスト名のIPアドレスを入力します。
`"<Message>"`	SNMP Trapテキストメッセージを指定します。

例 - 管理サーバからSNMP Trapを送信し、Security Gateway上のトラフィックをキャプチャする場合

```
[Expert@MGMT:0]# fwm snmp_trap -g 2 -c public 192.168.3.52 "My Trap Message"
[Expert@MGMT:0]#

[Expert@MyGW_192.168.3.52:0]# tcpdump -s 1500 -vvvv -i eth0 udp and host 192.168.3.51
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
22:49:43.891287 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: UDP (17), length: 103)
192.168.3.51.53450 > MyGW_192.168.3.52.snmptrap: [udp sum ok] { SNMPv1 { Trap(58) E:2620.1.1
192.168.3.240 linkDown 1486440 E:2620.1.1.11.0="My Trap Message" } }
CTRL+Cキー
[Expert@MyGW_192.168.3.52:0]#
```

fwm unload

説明

指定されたマネージドセキュリティゲートウェイまたはクラスタメンバからポリシーをアンロードします。

警告:

1. `fwm unload`コマンドは、指定したSecurity Gateway (クラスタメンバ) のLinuxカーネルでIP Forwardingを無効にするため、すべてのトラフィックがSecurity Gateway (クラスタメンバ) を通過するのを防ぎます。
2. `fwm unload`コマンドは、指定したSecurity Gateway (クラスタメンバ) からすべてのポリシーを削除します。
   つまり、セキュリティゲートウェイ(クラスタメンバ) が、フィルタリングや保護を有効にすることなく、すべてのアクティブなインタフェースを宛先とするすべての着信接続を受け入れます。

注:

- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- 現在のポリシーを削除し、セキュリティゲートウェイ(クラスタメンバ) は保護したままにする必要がある場合は、"`comp_init_policy`"コマンドをセキュリティゲートウェイ(クラスタメンバ) で実行します。
- Security Gateway(クラスタメンバ) にポリシーを読み込むには、Security Gateway (クラスタメンバ) 上で次のいずれかのコマンドを実行するか、再起動します。
  - "`fw fetch`"
  - "`cpstart`"

構文

```
fwm [-d] unload <GW1> <GW2> ... <GWN>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、`fwm`のsk97638プロセスの説明を参照してください。
<GW1> <GW2> ... <GWN>	SmartConsoleで設定したメインIPアドレスまたはオブジェクト名で、管理しているSecurity Gatewayを指定します。

例

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name: CXL_Policy
Policy install time: Wed Oct 23 18:23:14 2019
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 1
net.ipv6.conf.eth1.forwarding = 1
net.ipv6.conf.eth3.forwarding = 1
net.ipv6.conf.eth2.forwarding = 1
net.ipv6.conf.eth4.forwarding = 1
net.ipv6.conf.eth5.forwarding = 1
net.ipv6.conf.eth0.forwarding = 1
net.ipv6.conf.eth6.forwarding = 1
net.ipv6.conf.default.forwarding = 1
net.ipv6.conf.all.forwarding = 1
net.ipv6.conf.lo.forwarding = 1
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 1
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 1
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 1
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 1
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 1
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 1
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 1
[Expert@MyGW:0]#


[Expert@MGMT:0]# fwm unload MyGW

Uninstalling Policy From: MyGW

 Security Policy successfully uninstalled from MyGW...

Security Policy uninstall complete.

[Expert@MGMT:0]#
```

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name:
Policy install time:
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth3.forwarding = 0
net.ipv6.conf.eth2.forwarding = 0
net.ipv6.conf.eth4.forwarding = 0
net.ipv6.conf.eth5.forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth6.forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
[Expert@MyGW:0]#
```

fwm ver

説明

Security Management ServerのCheck Pointバージョンを表示します。

注 - マルチドメインサーバでは、このコマンドを実行することができます。

- MDSのコンテキストで

```
mdsenv
```

- ドメイン管理サーバのコンテキストで

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] ver [-f <Output File>]
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、`fwm`のsk97638プロセスの説明を参照してください。
`-f <Output File>`	この情報を保存する出力ファイル名を指定します。

例

```
[Expert@MGMT:0]# fwm ver
This is Check Point Security Management Server R82 - Build 11
[Expert@MGMT:0]#
```

fwm verify

重要 - このコマンドは、R80以降では使われていません。*mgmt_cli (978ページ)*コマンドを使用して、管理対象セキュリティゲートウェイでポリシーを検証します。

説明

指定されたポリシーパッケージをインストールせずに検証します。

注意
マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
fwm [-d] verify <Policy Name>
```

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。 完全なデバッグ手順については、`fwm`のsk97638プロセスの説明を参照してください。
<Policy Name>	SmartConsoleで設定されたポリシーパッケージの名前を指定します。

例

```
[Expert@MGMT:0]# fwm verify Standard
 Verifier messages:
Error: Rule 1 Hides rule 2 for Services & Applications: any .
[Expert@MGMT:0]#
```

inet_alert

説明

企業内ネットワークが攻撃されると、インターネットサービスプロバイダ(ISP) に通知します。このコマンドは、Check Point Security Gateway上のアラートデーモンによって生成されたログメッセージを外部の管理ステーションに転送します。この外部管理ステーションは、通常ISPサイトに設置されています。ISPはそのアラートを分析し、適切な対応をすることができます。

このコマンドは、Event Logging API(ELA) プロトコルを使用してアラートを送信します。アラートを受信する管理ステーションは、ELAプロキシを実行している必要があります。

ELAプロキシとの通信を認証または暗号化する場合は、ISPサイトでELAプロキシを実行している外部管理ステーションと、アラートを生成するCheck Point Security Gatewayとの間で鍵の交換を行う必要があります。

手順

ステップ	手順
1	SmartConsoleを使用して、外部の管理ステーションにログメッセージを転送するセキュリティゲートウェイを管理するSecurity Management ServerまたはDomain Management Serverに接続します。
2	左上のMenuから、Global propertiesをクリックします。
3	Log and Alertの近くにある[+]をクリックし、Alertsをクリックします。
4	Send user defined alert no. 1 to SmartView Monitorをクリアします。
5	オプションRun UserDefined script under the aboveを選択します。
6	該当するinet_alertアプリケーションを入力する(下記の*構文*セクションを参照) 。
7	クリックOK。
8	該当するSecurity Gatewayにアクセスコントロールポリシーをインストールします。

構文

```
inet_alert -s <IP Address> [-o] [-a <Auth Type>] [-p <Port>] [-f
<Token> <Value>] [-m <Alert Type>]
```

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

パラメータ

パラメータ	説明
`-s <IP Address>`	ELAプロキシのIPv4アドレス(通常ISPサイトに配置)。
`-o`	`stdout`に受信したアラートログを出力します。 このオプションは、`inet_alert`がパイプ構文(`<some command> | inet_alert ...`)の一部である場合に使用します。
`-a <Auth Type>`	ELAプロキシへの接続の種類を指定します。 次のうち1つの値になります。 ■ `ssl_opsec`- 接続は認証され、暗号化される(これがデフォルト)。 ■ `auth_opsec`- 接続は認証されている。 ■ `clear`- 接続は認証も暗号化もされていない。
`-p <Port>`	ELAプロキシのポート番号を指定します。デフォルトのポートは18187です。
`-f <Token> <Value>`	ログに追加するフィールド。以下のように`<Token> <Value>`のペアで表されます。 ■ `<Token>`- ログに追加するフィールドの名前。空白を含むことはできません。 ■ `<Value>`- フィールドの値。空白を含むことはできません。 このオプションを複数回使用すると、複数の`<Token> <Value>`ペアをログに追加することができます。

パラメータ	説明
-m <*Alert Type*>	ISPサイトで発生させるアラート。 このアラートは、アラートデーモンが生成するログメッセージで指定されたアラートより優先されます。 アラートに対する対応は、ISPセキュリティポリシーで設定されたアクションに従って処理されます。 これらのアラートは、OSのコマンドを実行するものです。 ■ alert- ポップアップ警告コマンド ■ mail- メールアラートコマンド ■ snmptrap- SNMPトラップ警告コマンド ■ spoofalert- なりすまし防止警告コマンド これらのNetQuotaとServerQuotaのアラートは、$FWDIR/conf/objects.C: ファイルに指定されたOSコマンドを実行します。 value=clientquotaalert. Parameter=clientquotaalertcmd

Existステータス

終了ステータス	説明
0	実行に成功しました。
102	未確定エラー。
103	メモリが割り当てられません。
104	ログ情報を取得できないstdin
106	コマンドラインの引数が無効です。
107	OPSEC APIの呼び出しに失敗しました。

例

```
inet_alert -s 10.0.2.4 -a clear -f product cads -m alert
```

このコマンドは、攻撃されたときにこれらの動作を行うように指定します。

- IPアドレス10.0.2.4に設置されたELAプロキシとのクリアな接続を確立します。
- 指定されたELAプロキシにログメッセージを送信します。このログメッセージのプロダクトフィールドを`cads`
- SmartConsole > **Menu > Global properties > Log and Alert > Popup Alert Command** フィールドで指定したOSコマンドをトリガする。

ldapcmd

説明

これらの機能を制御するLDAPユーティリティです。

機能	説明
キャッシュ	LDAPキャッシュの操作(キャッシュを空にする等)、およびデバッグ情報を提供します。
Statistics	次のような、LDAP検索の統計情報: ■ 全ユーザの検索 ■ ルックアップの保留(2つ以上のルックアップが同一である場合) ■ 検索の総合時間(特定の検索に要した総時間) ■ ヒット、ミスなどキャッシュの統計 これらの統計情報は、`$FWDIR/log/ldap_pid_<Process PID>.stats` ファイルに保存されます。
ログ記録	アラートログや警告ログを表示します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
ldapcmd [-d <Debug Level>] -p {<Process Name> | all} <Command>
```

パラメータ

パラメータ	説明
`-d <Debug Level>`	指定されたTDERRORデバッグレベルでデバッグモードでコマンドを実行します。 有効な値は0(無効)から5(最大レベル、推奨)。
`-p {<Process Name> | all}`	指定されたCheck Pointプロセス、またはサポートされているすべてのCheck Pointプロセスで実行されます。
`<Command>`	以下のいずれかのコマンドを実行します。 ■ `cacheclear {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all`- すべてのオブジェクトのキャッシュをクリア • `UserCacheObject`- ユーザオブジェクトのキャッシュをクリア • `TemplateCacheObject`- テンプレートオブジェクトのキャッシュをクリア • `TemplateExtGrpCacheObject`- 外部テンプレートグループオブジェクトのキャッシュをクリア ■ `cachetrace {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all`- すべてのオブジェクトのトレースキャッシュ • `UserCacheObject`- ユーザオブジェクトのトレースキャッシュ • `TemplateCacheObject`- テンプレートオブジェクトのトレースキャッシュ • `TemplateExtGrpCacheObject`- 外部テンプレートグループオブジェクトのトレースキャッシュ ■ `log {on | off}` • `on`- LDAPログの作成 • `off`- LDAPログを作成しない ■ `stat {<Print Interval in Sec> | 0}` • `<Print Interval in Sec>`- 統計の収集頻度 • `0`- 統計の収集を停止

ldapcompare

説明

これは、比較クエリを行い、その結果が一致するかどうかのメッセージを表示するLDAPユーティリティです。

このユーティリティは、LDAPディレクトリサーバへの接続を開き、バインドし、コマンドラインまたは指定されたファイルから指定された比較を実行します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
ldapcompare [-d <Debug Level>] [<Options>] <DN> {<Attribute>
<Value> | <Attribute> <Base64 Value>}
```

パラメータ

パラメータ	説明
`-d <Debug Level>`	指定されたTDERRORデバッグレベルでデバッグモードでコマンドを実行します。 有効な値は0(無効)から5(最大レベル、推奨)。
`<Options>`	以下の表をご覧ください。 ■ 比較オプション ■ 共通オプション
`<DN>`	識別名を指定します。
`<Attribute>`	アサーション属性を指定します。
`<Value>`	アサーション値を指定します。
`<Base64 Value>`	アサーション値のBase64エンコーディングを指定します。

比較オプション

オプション	説明
`-E [!]<Extension> [=<Extension Parameter>]`	比較拡張を指定します。 **注** - 感嘆符「！」は、重大性を示します。 例：`!dontUseCopy` = コピーを使用**しない**
`-M`	Manage DSA ITコントロールを有効にします。 クリティカルにするには"`-MM`"オプションを使用します。
`-P <LDAP Protocol Version>`	LDAPプロトコルのバージョンを指定します。デフォルトのバージョンは3です。
`-z`	クワイエットモードを有効にします。 このコマンドでは何も表示されません。コマンドの戻り値を利用することができます。

共通オプション

オプション	説明
`-D <Bind DN>`	LDAPサーバの管理者識別名を指定します。

オプション	説明
-e [!]<*Extension*> [=<*Extension Parameter*>]	一般的な拡張子を指定します。 **注** - 感嘆符「! 」は、重大性を示します。 ■ [!]assert=<*Filter*> RFC 4528; RFC 4515のフィルタ文字列 ■ [!]authzid=<*Authorization ID*> RFC 4370; "dn:<*DN*>"または"u:<*Username*>"のどちらか。 ■ [!]chaining[=<*Resolve Behavior*>[/<*Continuation Behavior*>]] いずれかの方法を実行します。 • "chainingPreferred" • "chainingRequired" • "referralsPreferred" • "referralsRequired" ■ [!]manageDSAit RFC 3296 ■ [!]noop ■ ppolicy ■ [!]postread[=<*Attributes*>] RFC 4527; カンマで区切られた属性のリスト ■ [!]preread[=<*Attributes*>] RFC 4527; カンマで区切られた属性のリスト ■ [!]relax ■ abandon SIGINTは放棄シグナルを送信し、クリティカルな場合はSIGINTを待たない。コントロールできない。 ■ cancel SIGINTはキャンセル信号を送信し、クリティカルな場合はSIGINTを待たない。コントロールできない。 ■ ignore SIGINTはレスポンスを無視し、クリティカルな場合はSIGINTを待たない。コントロールできない。
-h <*LDAP Server*>	LDAPサーバのコンピュータを、IPアドレスまたは解決可能なホスト名で指定します。
-H <*LDAP URI*>	LDAPサーバのURI(Uniform Resource Identifier) を指定します。
-I	SASL Interactiveモードを使用することを指定します。
-n	ドライラン - 何が行われるかを示し、実際には実行しません。

オプション	説明
`-N`	SASLホスト名の正規化にリバースDNSを使用しないことを指定します。
`-o <Option>[=<Option Parameter>]`	一般的なオプションを指定します。 `nettimeout={<Timeout in Sec> | none | max}`
`-O <Properties>`	SASLセキュリティのプロパティを指定します。
`-p <LDAP Server Port>`	LDAPサーバのポートを指定します。デフォルトは389です。
`-Q`	SASLクワイエットモードを使用することを指定します。
`-R <Realm>`	SASLレルムを指定します。
`-U <Authentication Identity>`	SASL認証のIDを指定します。
`-v`	冗長モードで実行する(診断結果を*標準出力*に表示)。
`-V`	バージョン情報を表示します("`-VV`"オプションのみを使用)。
`-w <LDAP Admin Password>`	LDAPサーバの管理者パスワードを指定します(簡易認証の場合)。
`-W`	LDAPサーバの管理者パスワードをユーザに入力させるかどうかを指定します。
`-x`	簡易認証を使用することを指定します。
`-X <Authorization Identity>`	SASL認証のIDを指定します(オプション"`dn:<DN>`"または"`u:<Username>`"のいずれか)。
`-y <File>`	LDAPサーバの管理者パスワードを`<File>`から読み取るように指定します。
`-Y <SASL Mechanism>`	SASLの仕組みを指定します。
`-Z`	TLSリクエストの開始を指定します。 "`-ZZ`"オプションを使用して、正常なレスポンスを要求できます。

ldapmemberconvert

説明

LDAPグループエントリの"Member"属性値から、LDAPメンバ(ユーザまたはテンプレート)エントリの"MemberOf"属性値へ移植するLDAPユーティリティです。

このユーティリティは、LDAPサーバのデータを"MemberOf"モード、または"Both"モードで動作するように変換するものです。このユーティリティは、1つ以上の"Member"属性値を保持する指定されたすべてのグループまたはテンプレート エントリを検索し、各値を変更します。このユーティリティは、指定されたすべてのグループ/テンプレート エントリを検索し、その"Member"属性値を取得します。

各値は、メンバエントリのDNです。このDNで識別されるエントリは、手元のグループ/テンプレートDNの"MemberOf"属性値に追加されます。さらに、このコマンドを"Both"モードで実行しない限り、グループ/テンプレートから"Member"属性値が削除されます。

このコマンドを実行すると、現在の作業ディレクトリにログファイル`ldapmemberconvert.log`が作成されます。このコマンドは、実行されたすべての変更と発生したエラーをそのログファイルに記録します。

重要- この変換ユーティリティを実行する*前*に、LDAPサーバデータベースをバックアップしてください。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
ldapmemberconvert [-d <Debug Level>] -h <LDAP Server> -p <LDAP
Server Port> -D <LDAP Admin DN> -w <LDAP Admin Password> -m
<Member Attribute Name> -o <MemberOf Attribute Name> -c <Member
ObjectClass Value> [-B] [-f <File> | -g <Group DN>] [-L <LDAP
Server Timeout>] [-M <Number of Updates>] [-S <Size>] [-T <LDAP
Client Timeout>] [-Z]
```

パラメータ

パラメータ	説明
`-d <Debug Level>`	指定されたTDERRORデバッグレベルでデバッグモードでコマンドを実行します。 有効な値は0(無効) から5(最大レベル、推奨) 。
`-h <LDAP Server>`	LDAPサーバのコンピュータを、IPアドレスまたは解決可能なホスト名で指定します。 LDAPサーバを明示的に指定しない場合、このコマンドは`localhost`に接続します。
`-p <LDAP Server Port>`	LDAPサーバのポートを指定します。デフォルトは389です。
`-D <LDAP Admin DN>`	LDAPサーバの管理者識別名を指定します。
`-w <LDAP Admin Password>`	LDAPサーバの管理者パスワードを指定します。
`-m <Member Attribute Name>`	グループ`Member`属性値を取得し、(場合によって) 削除する際のLDAP属性名を指定します。
`-o <MemberOf Attribute Name>`	LDAPの"`MemberOf`"属性値を追加する際のLDAP属性名を指定します。
`-c <Member ObjectClass Value>`	LDAPの"`ObjectClass`"属性値を指定します。この値は、変更するメンバの種類を定義します。 この構文では、複数の属性値を指定することができます。 `-c <Member Object Class 1> -c <Member Object Class 2> ... -c <Member Object Class N>`
`-B`	"`Both`"モードで実行することを指定します。

`-f <File>`	グループDNのリストを改行で区切って格納したファイルを指定します。
	`<Group DN 1>`
	`<Group DN 2>`
	`...`
	`<Group DN N>`
	1行の長さは256文字までです。

パラメータ	説明
`-g <Group DN>`	変換の対象となるグループまたはテンプレートの識別名を指定します。 この構文では、複数のグループDNを指定することができます。 `-g <Group DN 1> -g <Group DN 2> ... -g <Group DN N>`
`-L <LDAP Server Timeout>`	LDAP操作のサーバ側の時間制限を秒単位で指定します。 デフォルト値は`never`です。
`-M <Number of Updates>`	メンバLDAPの最大同時更新数を指定します。 デフォルトは20です。
`-S <Size>`	LDAP操作のサーバ側のサイズ制限をエントリ数で指定します。 デフォルト値は`none`です。
`-T <LDAP Client Timeout>`	LDAP操作のクライアント側のタイムアウトをミリ秒単位で指定します。 デフォルト値は`never`です。
`-Z`	SSL接続を使用することを指定します。

注

2つの"`GroupMembership`"モードがあります。これらのモードを統一しておく必要があります。

- `template-to-groups`
- `user-to-groups`

例えば、LDAPユーザに対して、そのグループの"`MemberOf`"属性を含むように変換を適用する場合、そのグループのLDAP定義テンプレートにもこの変換が適用されなければなりません。

トラブルシューティング

症状:

パラメータ-M <Number of Updates>を指定してコマンドを実行すると、接続が予期せず停止した旨のエラーメッセージが表示されて失敗します。

根本的な原因:

LDAPサーバは、同時に大量のLDAPリクエストを処理することができず、接続を終了しました。

解決策:

"-M"パラメータの値を小さくして、再度コマンドを実行します。デフォルトの値で大丈夫ですが、極端な状況では接続障害を引き起こす可能性もあります。コマンドが正常に実行されるまで、値を下げ続けてください。同じグループを使ってコマンドを実行するたびに、コマンドは中断したところから続行されます。

例

例1

グループは、DN "cn=cpGroup,ou=groups,ou=cp,c=us"と次の属性で定義されます。

```
...
cn=cpGroup
uniquemember="cn=member1,ou=people,ou=cp,c=us"
uniquemember="cn=member2,ou=people,ou=cp,c=us"
...
```

2つのメンバエントリの場合：

```
...
cn=member1
objectclass=fw1Person
...
```

および:

```
...
cn=member2
objectclass=fw1Person
...
```

次を実行します:

```
[Expert@MGMT:0]# ldapconvert -g cn=cpGroup,ou=groups,ou=cp,c=us -h MyLdapServer -d cn=admin -w secret -m uniquemember -o memberof -c
fw1Person
```

グループDNの結果：

```
...
cn=cpGroup
...
```

2つのメンバエントリの結果は、次のようになります。

```
...
cn=member1
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

および:

```
...
cn=member2
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

同じコマンドを"-B"パラメータで実行しても、同じ結果が得られますがグループエントリは変更されません。

例2

同じグループエントリに別のメンバ属性値が存在する場合：

```
uniquemember="cn=template1,ou=people, ou=cp,c=us"
```

テンプレート：

```
cn=member1
objectclass=fw1Template
```

その後、同じコマンドを実行すると、パラメータ"`-c fw1Person`"のために、テンプレートエントリはそのままですが、"`template1`"のオブジェクトクラスは"`fw1Template`"になっています。

ldapmodify

説明

LDAPサーバにユーザをインポートするLDAPユーティリティ。入力ファイルはLDIF形式である必要があります。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
ldapmodify [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Server Port>] [-D <LDAP Admin DN>] [-w <LDAP Admin Password>] [-a] [-b] [-c] [-F] [-k] [-n] [-r] [-v] [-T <LDAP Client Timeout>] [-Z] [ -f <Input File> .ldif | < <Entry>]
```

パラメータ

パラメータ	説明
`-d <Debug Level>`	指定されたTDERRORデバッグレベルでデバッグモードでコマンドを実行します。 有効な値は0(無効)から5(最大レベル、推奨)。
`-h <LDAP Server>`	LDAPサーバのコンピュータを、IPアドレスまたは解決可能なホスト名で指定します。 LDAPサーバを明示的に指定しない場合、このコマンドは`localhost`に接続します。
`-p <LDAP Server Port>`	LDAPサーバのポートを指定します。デフォルトは389です。
`-D <LDAP Admin DN>`	LDAPサーバの管理者識別名を指定します。
`-w <LDAP Admin Password>`	LDAPサーバの管理者パスワードを指定します。
`-a`	LDAP "`add`" 操作であることを指定します。

パラメータ	説明
`-b`	ファイルから値を読み込むことを指定します(バイナリ属性の場合) 。
`-c`	連続動作中のエラーを無視することを指定します。
`-F`	すべてのレコードに対して変更を強制することを指定します。
`-k`	Kerberosバインドを指定します。
`-K`	Kerberosバインド、パート1のみを指定します。
`-n`	LDAP"`add`"の操作を表示するように指定しますが、実際には実行されません。
`-r`	値を追加するのではなく、値を置き換えることを指定します。
`-v`	冗長モードで実行することを指定します。
`-T <LDAP Client Timeout>`	LDAP操作のクライアント側のタイムアウトをミリ秒単位で指定します。 デフォルト値は`never`です。
`-Z`	SSL接続を使用することを指定します。
`-f <Input File>.ldif`	`<Input File>.ldif`ファイルから読み込むことを指定します。 入力ファイルはLDIF形式である必要があります。
`< <Entry>`	*stdin*からエントリを読み込むことを指定します。 構文上、"<"文字は必須です。 入力が標準入力から(画面上に入力したデータから) 来ることを指定します。

ldapsearch

説明

LDAPディレクトリにクエリを行い、その結果を返すLDAPユーティリティです。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

```
ldapsearch [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Port>]
[-D <LDAP Admin DN>] [-w <LDAP Admin Password>] [-A] [-B] [-b
<Base DN>] [-F <Separator>] [-l <LDAP Server Timeout>] [-s
<Scope>] [-S <Sort Attribute>] [-t] [-T <LDAP Client Timeout>] [-
u] [-z <Number of Search Entries>] [-Z] <Filter> [<Attributes>]
```

パラメータ

パラメータ	説明
`-d <Debug Level>`	指定されたTDERRORデバッグレベルでデバッグモードでコマンドを実行します。 有効な値は0(無効)から5(最大レベル、推奨)。
`-h <LDAP Server>`	LDAPサーバのコンピュータを、IPアドレスまたは解決可能なホスト名で指定します。 LDAPサーバを明示的に指定しない場合、このコマンドは`localhost`に接続します。
`-p <LDAP Port>`	LDAPサーバのポートを指定します。デフォルトは389です。
`-D <LDAP Admin DN>`	LDAPサーバの管理者識別名を指定します。
`-w <LDAP Admin Password>`	LDAPサーバの管理者パスワードを指定します。
`-A`	属性名のみを取得し、値を取得しないことを指定します。
`-B`	非ASCII値の出力を抑制しないことを指定します。

パラメータ	説明
-b <*Base DN*>	検索用のベース識別名(DN)を指定します。
-F <*Separator*>	属性名とその値の間の出力区切り文字を指定します。 デフォルトの区切り文字は、等号(=)です。
-l <*LDAP Server Timeout*>	LDAP操作のサーバ側の時間制限を秒単位で指定します。 デフォルト値はneverです。
-s <*Scope*>	検索範囲を指定します。いずれかの方法を実行します。 ■ base ■ one ■ sub
-S <*Sort Attribute*>	この属性の値で結果をソートすることを指定します。
-t	/tmp/ディレクトリにあるファイルに値を書き込むことを指定します。 各 *<属性>-<値>*ペアを別々のファイルに書き出す: /tmp/ldapsearch-<*Attribute*>-<*Value*> 例えば、fw1color属性の値がa00188の場合、コマンドは次のファイルに書き込まれます: /tmp/ldapsearch-fw1color-a00188
-T <*LDAP Client Timeout*>	LDAP操作のクライアント側のタイムアウトをミリ秒単位で指定します。 デフォルト値: never
-u	出力にユーザフレンドリーなエントリ名を表示するよう指定します。 例: 表示cn=Babs Jensen, users, omi 代わりcn=Babs Jensen, cn=users,cn=omi
-z <*Number of Search Entries*>	LDAPサーバで検索するエントリの最大数を指定します。
-Z	SSL接続を使用することを指定します。
<*Filter*>	RFC-1558に準拠したLDAP検索フィルタ。 例: objectclass=fw1host
<*Attributes*>	取得する属性のリストを指定します。 属性を明示的に指定しない場合、コマンドはすべての属性を取得します。

例

```
[Expert@MGMT:0]# ldapsearch -p 18185 -b cn=omi objectclass=fw1host objectclass
```

この構文で、コマンドは

1. LDAPサーバに18185番ポートで接続します。
2. Base DN "`cn=omi`"で LDAP サーバに接続します。
3. LDAP ディレクトリに "`fw1host`"オブジェクトを照会します。
4. 見つかった各オブジェクトについて、その "`objectclass`"属性の値を表示します。

mgmt_cli

説明

mgmt_cliツールは、Management Server上の管理データベースと直接連動しています。

Gaia OS上で動作するManagement ServerまたはSecurity Gateway上の構文

```
mgmt_cli <Command Name> <Command Parameters> <Optional Switches>
```

Windows OS 32ビットで動作するSmartConsoleコンピュータでの構文

Windowsのコマンドプロンプトを開き、次のコマンドを実行します。

```
cd /d "%ProgramFiles%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional
Switches>
```

Windows OS 64ビットで動作するSmartConsoleコンピュータでの構文

Windowsのコマンドプロンプトを開き、次のコマンドを実行します。

```
cd /d "%ProgramFiles
(x86)%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional
Switches>
```

注

- mgmt_cliのオプションの完全なリストは、mgmt_cli (mgmt_cli.exe) コマンドを入力し、Enterを押してください。
- 詳細は次を参照: *Check Point Management API Reference*。

migrate

重要 - このコマンドは、R80.10およびそれ以下のバージョンから管理データベースを移行するために使用されます。
詳細は次を参照: *R82 Installation and Upgrade Guide*。

説明

管理データベースと適用可能なCheck Pointの設定をエクスポートします。

エクスポートされた管理データベースと適用可能なCheck Pointの設定をインポートします。

Management High Availability環境におけるバックアップと復元:

- 一貫性した環境をバックアップおよび復元するには、ハイアベイラビリティ環境内のすべてのサーバから同時にバックアップとスナップショットを収集し、復元するようにしてください。
- バックアップ操作が完了するまで、他の管理者がSmartConsoleで変更を加えないよう注意してください。

詳細:

- GaiaバックアップとGaiaスナップショットについては、次を参照: *R82 Gaia Administration Guide*。
- Virtual Machine Snapshotsについては、ベンダーのドキュメントを参照してください。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- 現在の管理データベースをバックアップする必要があり、より新しいソフトウェアバージョンを実行する管理サーバでインポートする予定が**ない**場合、`$FWDIR/bin/upgrade_tools/`ディレクトリの組み込みコマンドを使用することができます。
- 上位のソフトウェアバージョンを実行する管理サーバ上の管理データベースをインポートする予定の場合、その上位ソフトウェアバージョン用に特別に作成された移行ツールパッケージの`migrate`ユーティリティを使用する必要があります。その上位のソフトウェアバージョンについては、**インストール& アップグレードガイド**を参照してください。
- このコマンドが正常に終了した場合、このログファイルが作成されます。
  `/var/log/opt/CPshrd-R82/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  例: */var/log/opt/CPshrd-R82/migrate-2019.06.14_11.03.46.log*
- このコマンドが失敗した場合、このログファイルが作成されます。
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  例: */opt/CPshrd-R82/log/migrate-2019.06.14_11.21.39.log*

構文

- 組み込みのヘルプを表示するには

```
[Expert@MGMT:0]# ./migrate -h
```

- 管理データベースとコンフィギュレーションをエクスポートするには

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate export [-l | -x] [-n]
[--exclude-uepm-postgres-db] [--include-uepm-msi-files]
/<Full Path>/<Name of Exported File> &
```

- 管理データベースとコンフィギュレーションをインポートするには

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate import [-l | -x] [-n]
[--exclude-uepm-postgres-db] [--include-uepm-msi-files]
/<Full Path>/<Name of Exported File>.tgz &
```

パラメータ

パラメータ	説明
`-h`	組み込みのヘルプを表示します。
`yes | nohup ./migrate ... &`	この構文： 1. 対話型 "`migrate`"コマンドへの"`yes`"入力をパイプラインで送ります。 2. "`nohup`"は、"`migrate`"コマンドがシェルからのハングアップ信号を無視するように強制します。 3. "`&`"は、コマンドをバックグラウンドで実行することを強制します。 その結果、CLIセッションが終了しても、コマンドはバックグラウンドで実行され続けます。 次を参照してください。 ■ sk133312 ■ https://linux.die.net/man/1/bash ■ https://linux.die.net/man/1/nohup
`export`	管理データベースと適用可能なCheck Pointの設定をエクスポートします。
`import`	別の管理サーバからエクスポートされた管理データベースと該当するCheck Point設定をインポートします。

パラメータ	説明
`-l`	`$FWDIR/log/`ディレクトリにあるログインデックスを*含まない*Check Pointログをエクスポートおよびインポートします。 **重要:** ■ このコマンドはクローズドログ(現在情報が書き込まれていないログ)のみをエクスポートすることができます。 ■ このパラメータを使用すると、コマンドが完了するまでに長い時間がかかることがあります(ログの数による)。
`-x`	`$FWDIR/log/`ディレクトリにあるCheck Pointのログと*共に*そのインデックスをエクスポートおよびインポートします。 **重要:** ■ このパラメータは、Management Serverとログサーバの R80.10以降にのみ対応しています。 ■ このコマンドはクローズドログ(現在情報が書き込まれていないログ)のみをエクスポートすることができます。 ■ このパラメータを使用すると、コマンドが完了するまでに長い時間がかかることがあります(ログとインデックスの数による)。
`-n`	サイレント実行され(非インタラクティブモード)、各設定のデフォルトオプションが使用されます。 **重要:** ■ このモードで管理データベースをエクスポートし、エクスポートされたファイルの指定された名前が既存のファイルの名前と一致する場合、コマンドはプロンプトを表示せずに既存のファイルを上書きします。 ■ このモードで管理データベースをインポートすると、"`migrate import`"コマンドが自動的に"`cpstop`"コマンドを実行します。
`--exclude-uepm-postgres-db`	■ エクスポート操作の間、Endpoint Security Management ServerからPostgreSQLデータベースをバックアップしません。 ■ インポート操作の間、Endpoint Security Management Server上のPostgreSQLデータベースを復元しないようにします。
`--include-uepm-msi-files`	■ エクスポート操作の間、Endpoint Security Management ServerからMSIファイルをバックアップします。 ■ インポート操作の間、Endpoint Security Management Server上のMSIファイルを復元します。
/<Full Path>/	エクスポートされたデータベースファイルへの絶対パス。 このパスは必ず存在します。

パラメータ	説明
<Name of Exported File>	■ エクスポート操作の際に、出力ファイルの名前を指定します。このコマンドは、自動的に*.tgzという拡張子を追加します。 ■ インポート操作時に、エクスポートするファイル名を指定します。最後に*.tgzの拡張子を手動で入力する必要があります。

例1 - エクスポート操作に成功

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# ./migrate export /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R82/migrate-2019.06.14_11.03.46.log
[Expert@MGMT:0]#
```

例 2 - エクスポート操作に失敗

```
[Expert@MGMT:0]# ./migrate export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R82/log/migrate-2019.06.14_
11.21.39.log' for further details
[Expert@MGMT:0]#
```

migrate_server

重要 - このコマンドは、管理データベースを R80.20.M1、R80.20、R80.20.M2、R80.30、それ以上のバージョンから移行するために使用します。
詳細:

- sk135172 - Upgrade Tools
- 割り当てられたロールの*R82 Installation and Upgrade Guide*

説明

管理データベースと適用可能なCheck Pointの設定をエクスポートします。

エクスポートされた管理データベースと適用可能なCheck Pointの設定をインポートします。

Management High Availability環境におけるバックアップと復元:

- 一貫性した環境をバックアップおよび復元するには、ハイアベイラビリティ環境内のすべてのサーバから同時にバックアップとスナップショットを収集し、復元するようにしてください。
- バックアップ操作が完了するまで、他の管理者がSmartConsoleで変更を加えないよう注意してください。

詳細:

- GaiaバックアップとGaiaスナップショットについては、次を参照: *R82 Gaia Administration Guide*。
- Virtual Machine Snapshotsについては、ベンダーのドキュメントを参照してください。

注:

- このコマンドは、エキスパートモードから実行する必要があります。
- 現在の管理データベースをバックアップする必要があり、より新しいソフトウェアバージョンを実行する管理サーバでインポートする予定が**ない**場合、`$FWDIR/scripts/`ディレクトリの組み込みコマンドを使用することができます。
- 上位のソフトウェアバージョンを実行する管理サーバ上の管理データベースをインポートする予定の場合、その上位ソフトウェアバージョン用に特別に作成された移行ツールパッケージの`migrate_server`ユーティリティを使用する必要があります。その上位のソフトウェアバージョンについては、**インストール& アップグレードガイド**を参照してください。
- このコマンドが正常に終了した場合、このログファイルが作成されます。
`/var/log/opt/CPshrd-R82/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
例: */var/log/opt/CPshrd-R82/migrate-2022.06.14_11.03.46.log*
- このコマンドが失敗した場合、このログファイルが作成されます。
`$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
例: */opt/CPshrd-R82/log/migrate-2024-2025.06.14_11.21.39.log*

重要 - 現在の管理データベースをバックアップする必要があり、上位のソフトウェアバージョンを実行する管理サーバにインポートする予定が**ない**場合は、ソース管理サーバとターゲット管理サーバで同じJumbo Hotfix Accumulator Takeおよび他のすべてのプライベートHotfixが実行されていることを確認する必要があります。
インストールされたソフトウェアパッケージをすべて見るには次のコマンドを実行：`cpinfo -y all`

構文

- 組み込みのヘルプを表示するには

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server -h
```

- Pre-Upgrade Verifierを実行するには

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server verify -v R82 [-skip_
upgrade_tools_check]
```

- 管理データベースとコンフィギュレーションをエクスポートするには

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export -v R82 [-skip_
upgrade_tools_check] [-l | -x] [--include-uepm-msi-files] [--
exclude-uepm-postgres-db] [--ignore_warnings] /<Full
Path>/<Name of Exported File>
```

- 管理データベースとコンフィギュレーションをインポートするには

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server import -v R82 [-skip_
upgrade_tools_check] [-l | -x] [/var/log/mdss.json] [--
include-uepm-msi-files] [--exclude-uepm-postgres-db] /<Full
Path>/<Name of Exported File>.tgz
```

- Security Management Server上のDomain Management Serverデータベースと構成をインポートするには

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server migrate_import_domain -v
R82 [-skip_upgrade_tools_check] [-l | -x]
[/var/log/mdss.json] [--include-uepm-msi-files] [--exclude-
uepm-postgres-db] /<Full Path>/<Name of Exported File>.tgz
```

パラメータ

パラメータ	説明
`-h`	組み込みのヘルプを表示します。
`export`	管理データベースと適用可能なCheck Pointの設定をエクスポートします。

`import`	別の管理サーバからエクスポートされた管理データベースと該当するCheck Point設定をインポートします。
	重要:
	■ このコマンドは、Check Point サービスを自動的に再起動します("`cpstop`"および"`cpstart`"コマンドを実行)。
	■ これは、Multi-Domain Security Management環境において、少なくとも1つのサーバのIPv4アドレスが、データベースをエクスポートしたソースサーバと比較して変更された場合に適用されます。
	アップグレードとインポートを開始する**前に**、これらの手順を実行する必要があります。
	1. 新しいIPv4アドレスを含む特別なJSON設定ファイルを作成する必要があります。
	構文:
	`[{"name":"<Name of Server 1 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 1>"},`
	`{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]`
	例:
	`[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},`
	`{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]`
	2. このファイル**mdss.json**を呼び出す必要があります。
	3. このファイルは、**すべての**サーバで、ディレクトリ**/var/log/**に置く必要があります。

`migrate_import_domain`	Security Management Serverにおいて、Domain Management Serverからエクスポートされた管理データベースと該当するCheck Pointの設定をインポートします。 **重要** - このコマンドは、Check Pointサービスを自動的に再起動します("`cpstop`"および"`cpstart`"コマンドを実行)。

パラメータ	説明
`verify`	別の管理サーバからエクスポートされた管理データベースと適用可能なCheck Point構成を検証します。
`-v R82`	マイグレーション/アップグレード先のバージョンを指定します。
`-skip_upgrade_tools_check`	アップグレードツールの最新バージョンを確認するためにCheck Point Cloudに接続しようとしません。 **ベストプラクティス** - このパラメータは、インターネットに接続されて**いない**管理サーバで使用します。
`-l`	`$FWDIR/log/`ディレクトリにあるログインデックスを*含まない*Check Pointログをエクスポートおよびインポートします。 **重要:** ■ このコマンドはクローズドログ(現在情報が書き込まれていないログ)のみをエクスポートすることができます。 ■ このパラメータを使用すると、コマンドが完了するまでに長い時間がかかることがあります(ログの数による)。
`-x`	`$FWDIR/log/`ディレクトリにあるCheck Pointのログ*と共に*そのインデックスをエクスポートおよびインポートします。 **重要:** ■ このパラメータを使用する前に、すべてのログインデックスが閉じられ、保存されていることを確認する必要があります。 エキスパートモードでこのコマンドを実行し、出力に"`Solr stopped`"と表示されるのを待ちます。 `$RTDIR/scripts/stopSolr.sh` ■ このパラメータは、Management ServerとログサーバのR80.10以降にのみ対応しています。 ■ このコマンドはクローズドログ(現在情報が書き込まれていないログ)のみをエクスポートすることができます。 ■ このパラメータを使用すると、コマンドが完了するまでに長い時間がかかることがあります(ログとインデックスの数による)。

パラメータ	説明

`/var/log/mdss.json`	新しいIPv4アドレスを含む特殊なJSON設定ファイルへの絶対パスを指定します。
	パスとファイル名は必須です。
	このファイルは、Multi-Domain Security Management環境のアップグレード時に必須です。
	たとえ1台のサーバだけが新しいIPアドレスに移行しても、他のすべてのサーバはインポート処理のためにこの設定ファイルを取得する必要があります。
	構文:
	`[{"name":"<Name of Server 1 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 1>"},`
	`{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]`
	例:
	`[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},`
	`{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]`

`--include-uepm-msi-files`	■ エクスポート操作の間、Endpoint Security Management Serverから MSIファイルをバックアップします。 ■ インポート操作の間、Endpoint Security Management Server上の MSIファイルを復元します。
`--exclude-uepm-postgres-db`	■ エクスポート操作の間、Endpoint Security Management Serverから PostgreSQLデータベースをバックアップしません。 ■ インポート操作の間、Endpoint Security Management Server上の PostgreSQLデータベースを復元しないようにします。
`--ignore_warnings` または `-ivw`	アップグレード手順の途中でPre-Upgrade Verifierが警告を表示した場合、このパラメータを使用して警告を無視し、アップグレードを継続することができます。 **重要** - アップグレード中やアップグレード後の問題を防ぐために、このパラメータを使用せず、すべての問題を解決することを強くお勧めします。
`--exclude-licenses`	■ エクスポート操作の間、Management Serverからライセンスのバックアップを行いません。 ■ インポート操作の間、Management Serverのライセンスを復元しません。

パラメータ	説明

`--no_progress_bar`
または
`-npb`
	コマンドラインの進捗バーを無効にします。

`-n`	インタラクティブモードを無効にします。
/<Full Path>/<Name of Exported File>	エクスポートされたデータベースファイルの絶対パスを指定します。このパスは必ず存在します。 ■ エクスポート操作の際に、出力ファイルの名前を指定します。このコマンドは、自動的に`*.tgz`という拡張子を追加します。 ■ インポート操作時に、エクスポートするファイル名を指定します。最後に`*.tgz`の拡張子を手動で入力する必要があります。

例 1 - エクスポート操作に成功

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R82/migrate-2024 - 2025.06.14_11.03.46.log
[Expert@MGMT:0]#
```

例 2 - エクスポート操作に失敗

```
[Expert@MGMT:0]# ./migrate_server export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R82/log/migrate-2024 - 2025.06.14_
11.21.39.log' for further details
[Expert@MGMT:0]#
```

queryDB_util

説明

管理データベースでオブジェクトまたはポリシールールを検索します。

重要 - このコマンドは、R80以降では使われていません。*mgmt_cli (978ページ)*コマンドを使用して、検索パラメータに従ってオブジェクトまたはポリシールールを管理データベースから検索します。

rs_db_tool

説明

DAIPデータベースで動的割り当てIPアドレス(DAIP) ゲートウェイを管理します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

構文

- **DAIPデータベースにエントリを追加する:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation add -name <Object Name> -ip <IPv4 Address> -ip6 <Pv6 Address> -TTL <Time-To-Live>
```

- **DAIPデータベースから特定のエントリを取得する:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation fetch -name <Object Name>
```

- **DAIPデータベースから特定のエントリを削除する:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation delete -name <Object Name>
```

- **DAIPデータベースの全エントリをリストする:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation list
```

- **DAIPデータベースを同期させる:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation sync
```

注 - このコマンドは、エキスパートモードから実行する必要があります。

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-name <Object Name>`	DAIPオブジェクトの名前を指定します。
`-ip <IPv4 Address>`	DAIPオブジェクトのIPv4アドレスを指定します。
`-ip6 <IPv6 Address>`	DAIPオブジェクトのIPv6アドレスを指定します。
`-TTL <Time-To-Live>`	エントリが有効な相対的な間隔(秒)を指定します。

sam_alert

説明

SAM v1の場合、このユーティリティは標準入力から受け取った情報に従って、Suspicious Activity Monitoring (SAM) アクションを実行します。

SAM v2の場合、このユーティリティは、Suspicious Activity Monitoring(SAM) アクションをユーザ定義アラートメカニズムで実行します。

重要:

- このコマンドは、管理サーバ上で実行する必要があります。
- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

注:

- VSXゲートウェイとVSXクラスタメンバは、SAM(Suspicious Activity Monitoring) ルールをサポート**しません**。sk79700を参照してください。
- 詳細は*fw sam (885ページ)*と*fw sam_policy (894ページ)*コマンド。

SAM v1構文

```
sam_alert [-v] [-o] [-s <SAM Server>] [-t <Time>] [-f <Security
Gateway>] [-C] {-n|-i|-I} {-src|-dst|-any|-srv}
```

SAM v1のパラメータ

パラメータ	説明
`-v`	"`fw sam`"コマンドの詳細モードを有効にします。
`-o`	このツールの入力を標準出力に出力することを指定します(CLI 構文でパイプと一緒に使用するため) 。
`-s <SAM Server>`	連絡するSAMサーバを指定します。デフォルトは "localhost "です。
`-t <Time>`	アクションを実行する時間(秒) を指定します。デフォルトはforeverです。

パラメータ	説明
`-f <Security Gateway>`	操作を実行するセキュリティゲートウェイ/クラスタオブジェクトを指定します。 **重要** - 対象のセキュリティゲートウェイ/クラスタオブジェクトを明示的に指定しない場合、このコマンドは管理されているすべてのセキュリティゲートウェイとクラスタに適用されます。
`-C`	指定された操作を取り消します。
`-n`	セキュリティゲートウェイ/ClusterXL/セキュリティグループを通過するたびに通知します。
`-i`	指定された条件に一致する接続を禁止(ドロップまたは拒否)します。
`-I`	指定された条件に一致する接続を禁止(ドロップまたは拒否)し、指定された条件に一致する既存の接続をすべて閉じます。
`-src`	接続元アドレスにマッチします。
`-dst`	接続の宛先アドレスに一致します。
`-any`	接続元アドレスまたは接続先アドレスのいずれかに一致します。
`-srv`	特定の送信元、送信先、プロトコル、ポートに一致します。

SAM v2構文

```
sam_alert -v2 [-v] [-O] [-S <SAM Server>] [-t <Time>] [-f
<Security Gateway>] [-n <Name>] [-c "<Comment">] [-o
<Originator>] [-l {r | a}] -a {d | r| n | b | q | i} [-C] {-ip
|-eth} {-src|-dst|-any|-srv}
```

SAM v2のパラメータ

パラメータ	説明
`-v2`	SAM v2を使用することを指定します。
`-v`	"`fw sam`"コマンドの詳細モードを有効にします。
`-O`	このツールの入力を標準出力に出力することを指定します(CLI 構文でパイプと一緒に使用するため) 。
`-S <SAM Server>`	連絡するSAMサーバを指定します。デフォルトは "localhost "です。
`-t <Time>`	アクションを実行する時間(秒) を指定します。デフォルトはforever です。
`-f <Security Gateway>`	操作を実行するセキュリティゲートウェイ/クラスタオブジェクトを指定します。 **重要** - 対象のセキュリティゲートウェイ/クラスタオブジェクトを明示的に指定しない場合、このコマンドは管理されているすべてのセキュリティゲートウェイとクラスタに適用されます。
`-n <Name>`	SAMルールの名称を指定します。 デフォルトは空です。
`-c "<Comment>"`	SAMルールのコメントを指定します。 デフォルトは空です。 テキストは二重引用符または引用符で囲む必要があります。
`-o <Originator>`	SAMルールの発信元を指定します。 デフォルト値は`sam_alert`です。
`-l {r | a}`	指定した条件に一致する接続のログの種類を指定します。 ■ `r`- 標準 ■ `a`- アラート デフォルト値 : `None`

パラメータ	説明
`-a {d | r| n | b | q | i}`	指定された条件に一致する接続に適用するアクションを指定します。 ■ `d`- ドロップ ■ `r`- 拒否 ■ `n`- 通知 ■ `b`- バイパス ■ `q`- 隔離 ■ `i`- 検査
`-C`	条件に一致する既存の接続をすべて閉じることを指定します。
`-ip`	基準パラメータとしてIPアドレスを使用することを指定します。
`-eth`	MACアドレスを基準パラメータとして使用することを指定します。
`-src`	接続元アドレスにマッチします。
`-dst`	接続の宛先アドレスに一致します。
`-any`	接続元アドレスまたは接続先アドレスのいずれかに一致します。
`-srv`	特定の送信元、送信先、プロトコル、ポートに一致します。

例

sk110873: How to configure Security Gateway to detect and prevent port scanを参照してください。

stattest

説明

SNMP OIDを照会するCheck PointのAMONクライアント。

このコマンドは、デバッグ目的で標準のSNMPコマンドの代わりとして使用でき、該当するSNMP OIDが要求された情報を提供することを確認します。

注:

- このコマンドは、エキスパートモードでのみ実行可能です。
- マルチドメインサーバでは、該当するドメイン管理サーバのコンテキストでこのコマンドを実行する必要があります。

```
mdsenv <IP Address or Name of Domain Management Server>
```

標準OIDをクエリするための構文

- 管理サーバ/セキュリティゲートウェイ/クラスタメンバで:

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] [-v <VSID>] [-t <Timeout>] <Regular_OID_1> <Regular_OID_2> ...
<Regular_OID_N>
```

注:

- これらの標準OIDは、SNMP MIBファイルに指定されます。
- Check Point MIBファイルについては、sk90470を参照してください。

統計OIDをクエリするための構文

- 管理サーバ/セキュリティゲートウェイ/クラスタメンバで:

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] -l <Polling Interval> -r <Polling Duration> [-v <VSID>] [-t
<Timeout>] <Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>
```

注:

- これらの統計OIDは"初期化"に時間がかかります。
- 例えば、平均値を算出するためには、十分なサンプル数を集める必要があります。
- Check Pointの統計OIDは、`$CPDIR/conf/statistical_oid.conf`ファイルに登録されています。

パラメータ

パラメータ	説明
`-d`	デバッグモードでコマンドを実行します。 コマンド自体のトラブルシューティングを行う場合のみ使用します。 **ベストプラクティス** - このパラメータを使用する場合、出力をファイルにリダイレクトするか、`script`コマンドを使用してCLIセッション全体を保存してください。
`-h <Host>`	クエリするリモートのCheck Pointホストを、IPアドレスまたは解決可能なホスト名で指定します。
`-p <Port>`	AMONサーバがリッスンするポート番号を指定します。デフォルトのポートは18192です。
`-x <Proxy Server>`	プロキシサーバをIPアドレスまたは解決可能なホスト名で指定します。 **注** - リモートホストにクエリを実行するときのみ使用します。
`-l <Polling Interval>`	クエリ間の時間を秒単位で指定します。 **注** - 統計OIDのクエリを実行するときのみ使用します。
`-r <Polling Duration>`	連続したクエリを実行する時間を秒単位で指定します。 **注** - 統計OIDのクエリを実行するときのみ使用します。
`-t <Timeout>`	セッションタイムアウトをミリ秒単位で指定します。
`<Regular_OID_1> <Regular_OID_2> ... <Regular_OID_N>`	クエリを実行する標準OIDを指定します。 **注:** ■ OIDの先頭はピリオドであってはいけません。 ■ OIDはスペースで区切ってください。 ■ OIDは最大100個まで指定可能です。

パラメータ	説明
<Statistical_OID_1> *<Statistical_OID_2>* ... *<Statistical_OID_N>*	クエリを実行する統計OIDを指定します。 **注:** ■ OIDの先頭はピリオドであってはいけません。 ■ OIDはスペースで区切ってください。 ■ OIDは最大100個まで指定可能です。

例 - 標準OIDをクエリする

OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`)でCPUアイドル使用率をクエリします。

```
[Expert@HostName]# stattest get 1.3.6.1.4.1.2620.1.6.7.4.2
```

例 - 統計OIDをクエリする

OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`)でCPUアイドル使用率をクエリします。

5秒間の間に5秒間隔で情報を収集します。

```
[Expert@HostName]# stattest get -l 5 -r 5 1.3.6.1.4.1.2620.1.6.7.2.3
```

threshold_config

説明

SNMPトラップ(アラート) を発生させるさまざまなSNMPしきい値を設定することができます。

これらのしきい値を使用することで、各オブジェクトやデバイスに情報を要求することなく、多くのシステムコンポーネントを自動的に監視することができます。

SNMPモニタリングしきい値は、Security Management Server、Multi-Domain Server、またはDomain Management Serverでのみ設定できます。

ポリシーのインストール中、管理されたセキュリティゲートウェイとクラスタは、ポリシーの一部としてこれらのしきい値を受け取り、適用します。

詳細は、sk90860: How to configure SNMP on Gaia OSを参照してください。

手順

ステップ	手順
1	管理サーバのコマンドラインに接続します。
2	エキスパートモードにログインします。
3	マルチドメインサーバで、該当するドメイン管理サーバのコンテキストに切り替えます。 `[Expert@HostName:0]# mdsenv <Name or IP address of Domain Management Server>`
4	Threshold Engine Configurationメニューに移動します。 `[Expert@HostName:0]# threshold_config`

ステップ	手順

5	該当するオプションを選択し、該当の設定を行います
	(以下のThreshold Engine Configuration Optionsの表を参照)。
	`Threshold Engine Configuration Options:`
	`----------`
	`(1) Show policy name`
	`(2) Set policy name`
	`(3) Save policy`
	`(4) Save policy to file`
	`(5) Load policy from file`
	`(6) Configure global alert settings`
	`(7) Configure alert destinations`
	`(8) View thresholds overview`
	`(9) Configure thresholds`
	`(e) Exit (m) Main Menu`
	`Enter your choice (1-9) :`

6	Threshold Engine Configurationメニューを終了します。
7	CPDデーモンを停止します。 `[Expert@HostName:0]# cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"` 参照: *cpwd_admin stop (839ページ)*。
8	CPDデーモンを開始します。 `[Expert@HostName:0]# cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"` 参照: *cpwd_admin start (836ページ)*。
9	10 ~ 20秒待ちます。
10	CPDデーモンが正常に起動したことを確認します。 `[Expert@HostName:0]# cpwd_admin list | egrep "STAT|CPD"` 参照: *cpwd_admin list (832ページ)*。
11	SmartConsoleで、アクセスコントロールポリシーをセキュリティゲートウェイとクラスタにインストールします。

しきい値エンジン設定オプション

メニュー項目	説明
(1) Show policy name	現在設定されているしきい値ポリシーの名前を表示します。
(2) Set policy name	しきい値ポリシーの名前を設定します。 明示的に指定しない場合、デフォルトの名前は"Default Profile"です。
(3) Save policy	現在のしきい値ポリシーの変更内容を保存します。
(4) Save policy to file	設定されたしきい値ポリシーをファイルにエクスポートします。 明示的にパスを指定しない場合は、現在の作業ディレクトリに保存されます。
(5) Load policy from file	ファイルからしきい値ポリシーをインポートします。 明示的にパスを指定しない場合は、現在の作業ディレクトリからインポートされます。
(6) Configure global alert settings	グローバル設定を行います。 ■ アラートの送信頻度(30秒以上の遅延を設定すること) ■ アラート送信数

(7) Configure alert destinations	SNMPネットワーク管理システム(NMS)を設定し、管理対象のセキュリティゲートウェイとクラスタメンバがSNMPアラートを送信できるようにします。
	`Configure Alert Destinations Options:`
	`----------`
	`(1) View alert destinations`
	`(2) Add SNMP NMS`
	`(3) Remove SNMP NMS`
	`(4) Edit SNMP NMS`

(8) View thresholds overview	利用可能なすべてのしきい値とその現在の設定値のリストを表示します。これらは、以下のとおりです。 ■ 名前 ■ カテゴリ(次のオプション"(9)"を参照) ■ ステート(無効または有効) ■ しきい値(該当する場合しきい値ポイント) ■ 説明

メニュー項目	説明

(9) Configure thresholds	設定するしきい値カテゴリの一覧を表示します。
	`Thresholds Categories`
	`----------`
	`(1) Hardware`
	`(2) High Availability`
	`(3) Local Logging Mode Status`
	`(4) Log Server Connectivity`
	`(5) Networking`
	`(6) Resources`
	下記の**Thresholds Categories**の表をご覧ください。

しきい値のカテゴリ

カテゴリ	サブカテゴリ

(1) Hardware	`Hardware Thresholds:`
	`----------`
	`(1) RAID volume state`
	`(2) RAID disk state`
	`(3) RAID disk flags`
	`(4) Temperature sensor reading`
	`(5) Fan speed sensor reading`
	`(6) Voltage sensor reading`

(2) High Availability	`High Availability Thresholds:`
	`----------`
	`(1) Cluster member state changed`
	`(2) Cluster block state`
	`(3) Cluster state`
	`(4) Cluster problem status`
	`(5) Cluster interface status`

(3) Local Logging Mode Status	`Local Logging Mode Status Thresholds:`
	`----------`
	`(1) Local Logging Mode`

(4) Log Server Connectivity	`Log Server Connectivity Thresholds:`
	`----------`
	`(1) Connection with log server`
	`(2) Connection with all log servers`

カテゴリ	サブカテゴリ
(5) Networking	Networking Thresholds: ---------- (1) Interface Admin Status (2) Interface removed (3) Interface Operational Link Status (4) New connections rate (5) Concurrent connections rate (6) Bytes Throughput (7) Accepted Packet Rate (8) Drop caused by excessive traffic
(6) Resources	Resources Thresholds: ---------- (1) Swap Memory Utilization (2) Real Memory Utilization (3) Partition free space (4) Core Utilization (5) Core interrupts rate

注:

- セキュリティゲートウェイまたはクラスタメンバで`threshold_config`コマンドを*ローカル*に実行してSNMPモニタしきい値を設定した場合、ポリシーをインストールするたびにこれらの*ローカル*SNMPしきい値設定が消去され、このセキュリティゲートウェイまたはクラスタを管理するSecurity Management Serverで設定された*グローバル*SNMPしきい値設定に戻ります。
- Security Gatewayとクラスタメンバでは、ローカルのThreshold Engine Configurationの設定をファイルに保存して、後でローカルに読み込むことができます。
- Threshold Engine Configurationは、`$FWDIR/conf/thresholds.conf`ファイルに保存されます。
- Multi-Domain Security Management環境:
  - SNMPのしきい値は、マルチドメインサーバ(MDS)のコンテキストと、個々のドメイン管理サーバのコンテキストで設定することができます。
  - マルチドメインサーバのコンテキストで設定するしきい値は、マルチドメインサーバのみに適用されます。
  - ドメイン管理サーバのコンテキストで設定したしきい値は、そのドメイン管理サーバと、その管理下にあるセキュリティゲートウェイとクラスタのためのものです。
  - SNMPのしきい値がマルチドメインサーバとドメイン管理サーバの両方に適用される場合、マルチドメインサーバのコンテキストとドメイン管理サーバのカテゴリの両方でSNMPのしきい値を設定します。
    ただし、このシナリオでは、監視対象がしきい値を超えた場合のみ、マルチドメインサーバからアラートを受け取ることができます。
    例:
    CPUのしきい値を設定した場合、監視する値が設定したしきい値を超えると、マルチドメインサーバとドメイン管理サーバの両方に適用されます。ただし、SNMPアラートを生成するのはマルチドメインサーバのみです。

用語集

A

Anti-Virus (アンチウイルス)
セキュリティゲートウェイのCheck Point Software Blade。ThreatCloudが提供するリアルタイムのウイルスシグネチャとアノマリベースの防御機能により、ユーザが被害に遭う前にマルウェアを検出し、セキュリティゲートウェイでブロックする(略語 : AV) 。

C

CoreXL
マルチコア処理プラットフォーム上のセキュリティゲートウェイのパフォーマンスを向上させる技術。複数のCPUコア上で複数のCheck Pointファイアウォールインスタンスが並列動作する。

CoreXL SND
Secure Network Distributer。CoreXLの一部 : ネットワークインタフェースからの受信トラフィックの処理、許可されたパケットの安全な高速化 (SecureXLが有効な場合) 、ファイアウォールカーネルインスタンス間の非高速化パケットの分散 (SNDは、CoreXLファイアウォールインスタンスに割り当てられた接続をマッピングするグローバルディスパッチテーブルを維持) を担う。CoreXLファイアウォールインスタンス間のトラフィック分散は、ソースIPアドレス、宛先IPアドレス、およびIP「プロトコル」タイプに基づいて静的に行われる。CoreXL SNDはパケットに「触れる」ことはない。特定のFWKデーモンに固執するかどうかの決定は、他の何よりも前に、非常に高いレベルで接続の最初のパケットで行われる。SecureXLの設定にもよるが、多くの場合SecureXLは復号計算をオフロードすることができる。ただし、ルートベースのVPNのように、FWKデーモンによって復号計算が行われる場合もある。

CoreXL ファイアウォールインスタンス
CoreXLが有効なセキュリティゲートウェイでは、Firewallカーネルは複数回コピーされ、各コピー(ファイアウォールインスタンス) は、1つの処理CPUコアで実行される。ファイアウォールインスタンスは同時にトラフィックを処理し、各ファイアウォールインスタンスは完全で独立したファイアウォール検査カーネルとなる(同義語 : CoreXL FWインスタンス) 。

CPUSE
Gaiaオペレーティングシステム向けのCheck Point Upgrade Service Engine。CPUSEを使用すると、Gaia OS向けのCheck Point製品やGaia OS自体を自動的にアップグレードすることが可能。

D

DAIP ゲートウェイ
動的に割り当てられたIP(DAIP) セキュリティゲートウェイは、外部インタフェースのIPアドレスがISPによって動的に割り当てられるセキュリティゲートウェイです。

DLP (データ損失防止)
機密情報の外部への不正な送信を検知および防止する、セキュリティゲートウェイのCheck Point Software Blade(略語 : DLP) 。

E

Endpoint Policy Management
オンプレミスのHarmonyエンドポイントセキュリティ環境を管理するための管理サーバ上の Check Point Software Blade。

G

GAIA
SecurePlatformとIPSOオペレーティングシステムの両方の長所を組み合わせたCheckPoint セキュリティオペレーティングシステム。

Gaia Clish
Check Point Gaiaオペレーティングシステムのデフォルトのコマンドラインシェルの名前。制限付きシェル(ロールベースの管理により、シェルで使用できるコマンドの数が制御される) 。

Gaia Portal
Check Point Gaiaオペレーティングシステム用のWebインタフェース。

H

HTTPSインスペクション
SSL(Secure Sockets Layer) プロトコルによって暗号化されたトラフィックにマルウェアや不審なパターンがないか検査するセキュリティゲートウェイの機能(同義語 : SSLインスペクション、略語 : HTTPSI、HTTPSi) 。

I

ICA
内部認証局。認証用の証明書を発行する、Check Point Management Server上のコンポーネント。

IPS
さまざまなタイプのリスクについてパケットとデータを検査および分析するセキュリティゲートウェイ上のCheck Point Software Blade(侵入防止システム)。

IPsec VPN
サイト間VPNおよびリモートアクセスVPNアクセスを提供するセキュリティゲートウェイ上のCheck Point Software Blade。

J

Jumbo Hotfix Accumulator
Hotfixを1つのパッケージにまとめたもの(略語:JHA、JHF、JHFA)。

K

Kerberos
Microsoft Windows Active Directory Federation Services (ADFS)の認証サーバ。

M

Multi-Domain Server
ドメイン管理サーバと呼ばれる仮想Security Management Serverをホストする、Check Pointソフトウェアが動作するCheck Point専用サーバ(同義語:マルチドメインセキュリティ管理サーバ、略語:MDS)。

Q

QoS
セキュリティゲートウェイ上のCheck Point Software Bladeは、ポリシーベースのトラフィック帯域幅管理を提供し、ビジネスクリティカルなトラフィックに優先順位を付け、帯域幅を保証し、遅延を制御します。

S

SecureXL
セキュリティゲートウェイを通過するIPv4およびIPv6トラフィックを高速化するセキュリティゲートウェイ上のCheck Point製品。

Security Management Server
単一の管理ドメイン内でCheck Point環境のオブジェクトとポリシーを管理するために、Check Pointソフトウェアを実行するCheck Point専用サーバ(同義語 : Single-Domain Security Management Server) 。

SIC
セキュアな内部通信。Check Pointソフトウェアを実行するCheck Pointのコンピュータ同士がSSLを介して認証を行い、安全な通信を行うためのCheck Point独自の仕組み。Check Point Management Server上のICAが発行する証明書に基づいて認証される。

SmartConsole
Check Point 環境の管理に使用される Check Point GUI アプリケーション-セキュリティポリシーの構成、デバイスの構成、製品とイベントの監視、アップデートのインストールなど。

SmartDashboard
バージョンR77.30以前では、セキュリティ設定の作成と管理にレガシーなCheck Point GUIクライアントを使用しており、バージョンR80.X以降でも、特定のレガシー設定を構成するために使用される。

SmartProvisioning
設定プロファイルを使用してCheck Pointセキュリティゲートウェイの大規模なデプロイメントを管理する、管理サーバ(実際の名称は「Provisioning」) 上のCheck Point Software Blade (同義語 : 大規模管理、SmartLSM、LSM) 。

SmartUpdate
Check Point環境でライセンスと契約を管理するために使用されるレガシーCheck Point GUIクライアント。

Software Blade
特定のセキュリティソリューション(モジュール) : (1) セキュリティゲートウェイでは、各Software Bladeがトラフィックの特定の特性を検査する (2) 管理サーバでは、各Software Bladeが異なる管理機能を有効にする。

T

Threat Emulation
サンドボックス内のファイル動作をモニタし、悪意のあるファイルかどうかを判断するセキュリティゲートウェイのCheck Point Software Blade(略語:TE)。

Threat Extraction
ファイルから悪意のあるコンテンツを削除するセキュリティゲートウェイのCheck Point Software Blade(略語:TEX)。

U

URLフィルタリング
セキュリティゲートウェイ上のCheck Point Software Bladeで、特定のユーザグループ、コンピュータ、またはネットワークからアクセス可能なWebサイトをきめ細かく制御することができる(略語:URLF)。

V

VSX
Virtual System Extension。Check Pointの仮想ネットワークソリューションであり、コンピュータまたはクラスタ上でホストされ、Check Pointのセキュリティゲートウェイやその他のネットワークデバイスを仮想的に抽象化したもの。仮想デバイスは、物理デバイスと同等の機能を提供する。

VSXゲートウェイ
物理ネットワークデバイスの機能を提供する全てのバーチャルデバイスを含む、VSXバーチャルネットワークをホストする物理サーバ。VS0と呼ばれる少なくとも1つの仮想システムを保持する。

あ

アイデンティティロギング
管理サーバのCheck Point Software Bladeを有効にして、ID認識ソフトウェアブレードが有効になっている管理対象セキュリティゲートウェイからのIDログを表示します。

アイデンティティアウェアネス
セキュリティゲートウェイのCheck Point Software Blade。ネットワークの場所、ユーザのID、コンピュータの識別情報に基づいて、ネットワークアクセスを強制し、データを監査する(略語 : IDA) 。

アクティブSecurity Management Server
現在アクティブに設定されているManagement High AvailabilityのManagement Server。

アプリケーション コントロール
ディープパケットインスペクションにより、特定のWebアプリケーションをきめ細かく制御できる、セキュリティゲートウェイのCheck Point Software Blade(略語 : APPI) 。

アンチスパム
Eメールの検査に包括的な保護を提供するセキュリティゲートウェイのCheck Point Software Blade(同義語 : アンチスパム& メールセキュリティ、略語 : AS、ASPAM) 。

アンチボット
ボットネットの動作とコマンド & コントロール(C&C) センターへの通信を遮断する、セキュリティゲートウェイのCheck Point Software Blade(略語AB、ABOT) 。

い

インラインレイヤ
セキュリティポリシーの別のルールで使用されるルールのセット。

え

エキスパートモード
CheckPoint Gaiaオペレーティングシステムで完全なシステムルート権限を付与する完全なコマンドラインシェルの名前。

お

オープンサーバ
Check Point以外の会社によって製造、配布されている物理コンピュータ。

く

クラスタ
冗長構成で連携する2つ以上のセキュリティゲートウェイ(ハイアベイラビリティまたは負荷分散)をクラスタ化します。

クラスタ メンバ
クラスタの一部であるセキュリティゲートウェイ。

こ

コンテンツアウェアネス
データの可視化とエンフォースを行うセキュリティゲートウェイのCheck Point Software Blade(略語:CTNT)。

コンプライアンス
管理対象のセキュリティゲートウェイにセキュリティベストプラクティスを表示および適用する、管理サーバ上のCheck Point Software Blade。このSoftware Bladeには、Check Point定義のセキュリティベストプラクティスのライブラリが含まれており、セキュリティゲートウェイとポリシーを適切に設定するためのベースラインとして使用可能。

す

スタンドアロン
Security Gatewayとセキュリティマネジメントサーバ製品が同じサーバにインストールされ、設定される構成。

スタンバイSecurity Management Server
現在スタンバイとして設定されているManagement High AvailabilityのSecurity Management Server。

せ

セカンダリSecurity Management Server
セカンダリとしてインストールするManagement High AvailabilityのSecurity Management Server。

セキュリティゲートウェイ
Check Pointソフトウェアを実行してトラフィックを検査し、接続されたネットワークリソースにセキュリティポリシーを適用する専用Check Pointサーバ。

セキュリティポリシー
ネットワークトラフィックを制御し、データ保護とパケット検査によるリソースへのアクセスに関する組織のガイドラインを適用するルールのコレクション。

ゼロフィッシング
URLに基づくリアルタイムのフィッシング対策を提供する、R81.20以降のセキュリティゲートウェイのCheck Point Software Blade(略語:ZPH)。

た

ダイナミックオブジェクト
IPアドレスが事前にわからない特殊なオブジェクトタイプ。セキュリティゲートウェイはこのオブジェクトのIPアドレスをリアルタイムで解決する。

て

データタイプ
コンテンツ認識ソフトウェアブレードのCheck Pointセキュリティポリシーにおけるデータの分類。

ね

ネットワークオブジェクト
企業トポロジのさまざまな部分(コンピュータ、IPアドレス、トラフィックプロトコルなど)を表す論理オブジェクト。管理者はこれらのオブジェクトをセキュリティポリシーで使用する。

ネットワークポリシー管理
管理サーバ上のCheck Point Software Bladeを使用して、アクセス制御および脅威防止ポリシーを使用してオンプレミス環境を管理します。

は

ハイアベイラビリティ(HA) 管理
2 台のCheck Point管理サーバを配置・構成するモードで、管理データベースを自動的に同期させます。このモードでは、一方の管理サーバがアクティブ、もう一方の管理サーバがスタンバイとなる。略語 : Management HA、MGMT HA。

パッケージリポジトリ
管理サーバーにアップロードされたソフトウェアパッケージのコレクションです。これらのパッケージは、SmartConsoleで管理対象のセキュリティゲートウェイに簡単にインストールできます。

ふ

プライマリSecurity Management Server
プライマリとしてインストールしたManagement High AvailabilityのSecurity Management Server。

ブリッジモード
既存のトポロジに簡単に展開できるレイヤ2ブリッジデバイスとして機能するセキュリティゲートウェイまたは仮想システム。

プロビジョニング
設定プロファイルを使用してCheck Pointセキュリティゲートウェイの大規模なデプロイメントを管理する、管理サーバ上のCheck Point Software Blade(同義語 : SmartProvisioning、SmartLSM、Large-Scale Management、LSM) 。

ほ

ホットフィックス
誤った動作や望ましくない動作を修正し、新しい動作を追加するために、現在のソフトウェアバージョンにソフトウェアパッケージをインストールします。

ポリシーパッケージ
アクセス・コントロール、脅威対策、QoS、デスクトップ・セキュリティなど、さまざまなタイプのセキュリティ・ポリシーのコレクション。インストール後、セキュリティゲートウェイはポリシーパッケージ内のすべてのポリシーを実施します。

ポリシーレイヤー
セキュリティポリシーのレイヤー(ルールの集合) 。

ま

マルチドメイン・ログ・サーバ
マルチドメインセキュリティ管理環境におけるログの保存と処理を行う、Check Pointソフトウェアを実行するCheck Point専用サーバ。マルチドメイン ログサーバはドメインログサーバで構成され、対応するドメイン管理サーバによって管理されるセキュリティゲートウェイからのログを保存および処理する(略語 : MDLS) 。

も

モバイルアクセス
管理下および非管理下のクライアントにリモートアクセスVPNアクセスを提供する、セキュリティゲートウェイのCheck Point Software Blade(略語 : MAB) 。

ゆ

ユーザグループ
関連する責任を持つユーザの名前付きグループ。

ユーザディレクトリ
LDAP およびその他の外部ユーザ管理サーバを Check Point 製品およびセキュリティソリューションと統合する管理サーバ上の Check Point Software Blade。

ユーザデータベース
スマートコンソールで定義および管理されるすべてのユーザを含むCheck Point内部データベース。

ユーザテンプレート
セキュリティ ポリシーを適用するユーザの種類を定義するプロパティセット 。

る

ルール
通信セッションに対して指定されたアクションが実行されるようにする、ルールベース内のトラフィックパラメータおよびその他の条件のセット 。

ルールベース
特定のセキュリティポリシーに設定されたすべてのルール(同義語 : ルールベース) 。

ろ

ロギングとステータス
管理サーバ上のCheck Point Software Bladeで、管理対象のセキュリティゲートウェイからのセキュリティログを表示します。

ログ サーバ
Check Pointソフトウェアを実行してログを保存および処理する専用Check Pointサーバ。

漢字

監査ログ
管理サーバに対する管理者アクション (ログインとログアウト、オブジェクトの作成または変更、ポリシーのインストールなど) を含むログ。

管理インタフェース
(1) Gaia Security Gatewayまたはクラスタメンバ上のインタフェース。(2) Gaiaコンピュータ上のインタフェースで、ユーザがGaia PortalまたはCLIに接続するためのもの。

管理サーバ
Check Point シングルドメインセキュリティ管理サーバまたはマルチドメインセキュリティ管理サーバ。

権限プロファイル
ドメインと管理者に割り当てられたSmartConsoleのアクセス許可の定義済みグループです。この機能を使用すると、1つの定義で多くの管理者に複雑なアクセス許可を設定できます。

更新可能オブジェクト
Microsoft 365、AWS、ジオロケーションなどの外部サービスを表すネットワークオブジェクト。

手動 NAT ルール
Check Point管理サーバの管理者によるNATルールの手動構成。

内部ネットワーク
ファイアウォールによって保護され、認証されたユーザによってアクセスされるコンピュータとリソース。

分散展開
Check Point Security Gateway とSecurity Management Server製品が別のコンピュータにインストールされている構成。