

QUANTUM

22 April 2024

QUANTUM MAESTRO

R80.20SP

Administration Guide

CHECK POINT™

Check Point Copyright Notice

© 2019 - 2024 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

Important Information



Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.



Check Point R80.20SP Quantum Maestro Administration Guide

For more about this release, see the R80.20SP home page.



Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.



Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
26 November 2023	Added: ■ *"Configuring VLAN Interfaces on Uplink Ports" on page 124* Updated: ■ *"Installing a Hotfix Package on Orchestrators" on page 351* - CPUSE online installation is not supported ■ *"Clean Install of the Gaia Image on an Orchestrator with a Bootable USB Device" on page 458* ■ *"Log Server Distribution (asg_log_servers, set / show smo log-distribution)" on page 316* ■ *"Summary of Configuration Options" on page 40* ■ *"Viewing VLAN Interfaces on Uplink Ports" on page 74* Removed: ■ "Working with Session Control (asg_session_control)" - this command is not supported ■ *"Configuring Security Groups in Gaia Clish" on page 56* - removed deprecated procedures: • Adding VLAN Interfaces on Uplink Ports • Removing VLAN Interfaces from Uplink Ports
01 October 2023	Updated: ■ *"Troubleshooting" on page 438*
07 April 2023	Updated: ■ *"Configuring Security Groups in Gaia Portal" on page 44* - Best Practice about enabling the SMO Image Cloning ■ *"Configuring Security Groups in Gaia Clish" on page 56* - Best Practice about enabling the SMO Image Cloning ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 354*
04 April 2023	Updated: ■ *"Multi-blade Traffic Capture (tcpdump -mcap, tcpdump -view)" on page 217*
26 February 2023	Updated: ■ *"Configuring Bond Interface on Uplink Ports" on page 109*

Date	Description
02 February 2023	Updated: ■ *"Policy Management on Security Group Members" on page 27*
11 January 2023	Updated: ■ *"IP Block Feature" on page 374*
18 December 2022	Updated: ■ *"General Diagnostic in Security Groups" on page 444*
13 December 2022	Updated: ■ *"General Diagnostic in Security Groups" on page 444*
01 December 2022	Updated: ■ Starting from the R80.20SP Jumbo Hotfix Accumulator Take 304 on the Quantum Maestro Orchestrator, it is **not** necessary to configure VLAN interfaces on Uplink ports: • *"Configuring Security Groups in Gaia Portal" on page 44* • *"Configuring Security Groups in Gaia Clish" on page 56*
17 October 2021	Added: ■ *"Configuring Services to Synchronize After a Delay" on page 336* ■ *"Forwarding specific inbound-connections to the SMO (asg_excp_conf)" on page 340* Updated: ■ *"Configuring Alerts for Security Group Member and Security Group Events (asg alert)" on page 286*
15 October 2021	Updated: ■ *"Configuring Security Groups in Gaia Clish" on page 56* - added important notes about the "`admin-state`" parameter
28 June 2021	Updated: ■ *"Replacing a Quantum Maestro Orchestrator" on page 459*
13 June 2021	Removed (temporarily): ■ *"Replacing a Quantum Maestro Orchestrator" on page 459*

Date	Description
17 May 2021	Improved: ■ Formatting and document layout Added: ■ *"Policy Management on Security Group Members" on page 27* ■ *"Backing Up and Restoring Gaia Configuration" on page 154* ■ *"Configuring Security Groups" on page 35* ■ *"Deploying a Security Group in Monitor Mode" on page 383* ■ *"Deploying a Security Group in Bridge Mode" on page 418* Updated: ■ *"Working with the Distribution Mode" on page 159* ■ *"IPS Management During a Cluster Failover" on page 187* ■ *"Monitoring Performance (asg perf)" on page 223* ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 354*
18 February 2020	Updated: ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 354* - removed the steps for "Online CPUSE packages"
07 January 2020	Added: ■ *"IP Block and URL Block Features" on page 374* ■ *"Configuring Security Group High Availability" on page 372* Updated: ■ *"Packet Drop Monitoring (drop_monitor and asg_drop_monitor)" on page 258* ■ *"Monitoring Bond Interfaces (asg_bond)" on page 195* ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 354*
12 August 2019	Updated: ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 354* • Added instructions for installation of CPUSE Online packages • Removed the section *Deleting a Hotfix Package* as not supported

Date	Description
06 August 2019	Updated: ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 354*: • Updated the Important Notes about dividing all Security Group Members in a specific Security Group into two logical groups • Added the Important Notes about connection over the serial console
04 August 2019	Updated: ■ *"Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators" on page 350* - added a note that upgrade of CPUSE Agent is not supported ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 354* - added a note that upgrade of CPUSE Agent is not supported
01 July 2019	Updated: ■ Document design Removed: ■ Information about initial configuration was moved to the R80.20SP Maestro Getting Started Guide: • Connecting Cables to Quantum Maestro Orchestrators • Configuration Procedure • License Installation • Managing Security Groups (some topics) Added: ■ *"Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators" on page 350* ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 354* ■ *Replacing a Quantum Maestro Orchestrator*
24 March 2019	Updated: ■ Breakout Cables

Date	Description
17 March 2019	Updated: ■ Connecting Two Quantum Maestro Orchestrators for Redundancy ■ Connecting Cables to MHO-170 ■ Connecting Cables to MHO-140 ■ Summary of Configuration Options ■ Special Scenarios ■ License Installation ■ Snapshot Management ■ Log and Configuration Files Added: ■ Installing the Gaia Operating System on a Quantum Maestro Orchestrator ■ General Diagnostic in Security Groups
28 February 2019	First release of this document

Table of Contents

Introduction ... *17*
Important Links ... *17*
Security Group Concepts ... *18*
Single Management Object (SMO) and Policies ... *18*
Single Management Object ... *19*
Installing and Uninstalling Policies ... *22*
Working with Policies (asg policy) ... *23*
Policy Management on Security Group Members ... *27*
Synchronizing Policy and Configuration Between Security Group Members ... *28*
Understanding the Configuration File List ... *29*
MAC Addresses and Bit Conventions ... *31*
MAC Address Resolver (asg_mac_resolver) ... *34*
Configuring Security Groups ... *35*
Workflow ... *35*
Configuration Procedure ... *38*
Workflow for Configuring Security Groups ... *38*
Summary of Configuration Options ... *40*
Configuring Security Groups in Gaia Portal ... *44*
Configuring Security Groups in Gaia Clish ... *56*
Configuring Gaia Settings of a Security Group ... *91*
Configuration in SmartConsole ... *93*
Special Configuration Scenarios ... *105*
Configuring Bond Interface on the Management Ports ... *105*
Configuring Bond Interface on Uplink Ports ... *109*
Configuring VLAN Interfaces on top of a Bond Interface on Uplink Ports ... *115*
Procedure ... *115*
Example ... *120*

Configuring VLAN Interfaces on Uplink Ports ... 124
Introduction ... 124
Viewing VLAN Interfaces on Uplink Ports in Gaia Portal ... 125
Viewing VLAN Interfaces on Uplink Ports in Gaia Clish ... 126
Configuring More Than 4000 VLAN Interfaces on Orchestrators ... 127
License Installation ... 129
Managing Security Groups ... 131
Connecting to a Specific Security Group Member (member) ... 131
Global Commands ... 134
Working with Global Commands ... 135
General Global Commands ... 136
Global Operating System Commands ... 144
Check Point Global Commands ... 151
Backing Up and Restoring Gaia Configuration ... 154
Working with Security Group Gaia gClish Configuration (asg_config) ... 155
Configuring Security Group Members (asg_blade_config) ... 157
Working with the Distribution Mode ... 159
Background ... 159
Automatic Distribution Configuration (Auto-Topology) ... 160
Manual Distribution Configuration (Manual-General) ... 160
Setting and Showing the Distribution Configuration (set distribution configuration) ... 161
Configuring the Interface Distribution Mode (set distribution interface) ... 163
Showing Distribution Status (show distribution status) ... 165
Running a Verification Test (show distribution verification) ... 167
Configuring the Layer 4 Distribution Mode and Masks (set distribution l4-mode) ... 168
Configuring the Cluster State (g_clusterXL_admin) ... 170
Configuring a Unique MAC Identifier (asg_unique_mac_utility) ... 173
Background ... 173
Configuring the Unique MAC Identifier Manually ... 174
Options of the Unique MAC Identifier Utility ... 174

Working with the ARP Table (asg_arp) 176
The 'asg_arp' Command 177
Example Default Output 179
Example Verbose Output 180
Example Output for Verifying MAC Addresses 180
Verifying ARP Entries 180
Example Legacy Output 181
Working with the GARP Chunk Mechanism 182
Description 182
Configuration 183
Verification 184
NAT and the Correction Layer on a VSX Gateway 185
NAT and the Correction Layer on a Security Gateway 186
IPS Management During a Cluster Failover 187
IPv6 Neighbor Discovery 188
Logging and Monitoring 189
CPView 189
Overview of CPView 189
CPView User Interface 189
Using CPView 190
Network Monitoring 191
Working with Interface Status (asg if) 191
Global View of All Interfaces (show interfaces) 194
Monitoring Bond Interfaces (asg_bond) 195
Viewing a Global List of All Bond Interfaces (asg_bond) 196
Viewing a Specific Bond Interface (asg_bond -i) 196
Running a Bond Verification Test (asg_bond -v) 197
Monitoring Traffic (asg_ifconfig) 198
Monitoring Multicast Traffic 206
Showing Multicast Routing (asg_mroute) 206

Showing PIM Information (asg_pim) ... 209
Showing IGMP Information (asg_igmp) ... 212
Monitoring VPN Tunnels ... 215
SmartConsole ... 215
SNMP ... 215
CLI Tools ... 215
Traceroute (asg_tracert) ... 216
Multi-blade Traffic Capture (tcpdump -mcap, tcpdump -view) ... 217
Monitoring Management Interfaces Link State ... 220
Performance Monitoring and Control ... 222
Monitoring Performance (asg perf) ... 223
Performance Hogs (asg_perf_hogs) ... 239
Syntax ... 239
Configuration ... 240
The [tests] Section ... 241
Setting Port Priority ... 249
Searching for a Connection (asg search) ... 250
Description ... 250
Searching in the Non-Interactive Mode ... 250
Searching in the Interactive Mode ... 254
Showing the Number of Firewall and SecureXL Connections (asg_conns) ... 256
Packet Drop Monitoring (drop_monitor and asg_drop_monitor) ... 258
The "drop_monitor" command ... 258
The "asg_drop_monitor" command ... 262
Hardware Monitoring and Control ... 264
Showing Hardware State (asg stat) ... 264
Monitoring System and Component Status (asg monitor) ... 274
Configuring Alert Thresholds (set chassis alert_threshold) ... 276
Monitoring System Resources (asg resource) ... 279

Configuring Alerts for Security Group Member and Security Group Events (asg alert) ... 286
Collecting System Diagnostics (smo verifiers) ... 290
Diagnostic Tests ... 290
Showing the Tests ... 292
Showing the Last Run Diagnostic Tests ... 293
Running all Diagnostic Tests ... 294
Running Specific Diagnostic Tests ... 295
Collecting Diagnostic Information for a Report Specified Section ... 297
Error Types ... 298
Changing Compliance Thresholds ... 299
Changing the Default Test Behavior of the 'asg diag resource verifier' ... 299
Troubleshooting Failures ... 301
Alert Modes ... 305
Diagnostic Events ... 305
Important Notes ... 306
Known Limitations of the SMO Verifiers Test ... 310
System Monitoring ... 311
Showing System Serial Numbers (asg_serial_info) ... 311
Showing the Security Group Version (ver) ... 312
Showing System Messages (show smo log) ... 313
Configuring a Dedicated Logging Port ... 314
Log Server Distribution (asg_log_servers, set / show smo log-distribution) ... 316
Command Auditing (asg log audit) ... 319
Viewing a Log File (asg log) ... 320
Monitoring Virtual Systems (cpha_vsx_util monitor) ... 323
Software Blades Update Verification (asg_swb_update_verifier) ... 324
Working with SNMP ... 328
Monitoring Quantum Maestro Orchestrators over SNMP ... 328
Enabling SNMP Monitoring on Quantum Maestro Orchestrators ... 328

Supported SNMP OIDs for Quantum Maestro Orchestrators ... 329
Supported SNMP Trap OIDs for Quantum Maestro Orchestrators ... 330
Monitoring Security Groups over SNMP ... 331
Enabling SNMP Monitoring of Security Groups ... 331
Supported SNMP OIDs for Security Groups ... 332
Supported SNMP Trap OIDs for Security Groups ... 332
SNMP Monitoring of Security Groups in VSX Mode ... 332
Common SNMP OIDs for Security Groups ... 333
System Optimization ... 336
Configuring Services to Synchronize After a Delay ... 336
Firewall Connections Table Size for VSX Gateway ... 339
Forwarding specific inbound-connections to the SMO (asg_excp_conf) ... 340
Installing and Uninstalling a Hotfix ... 350
Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators ... 350
Installing a Hotfix Package on Orchestrators ... 351
Uninstalling a Hotfix Package on Orchestrators ... 353
Deleting a Hotfix Package on Orchestrators ... 353
Installing and Uninstalling a Hotfix on Security Group Members ... 354
Installing a Hotfix Package on Security Group Members ... 355
Uninstalling a Hotfix Package on Security Group Members ... 365
Configuring Security Group High Availability ... 372
Setting Security Group Weights (High Availability Factors) ... 372
Setting the Quality Grade Differential ... 373
IP Block and URL Block Features ... 374
IP Block Feature ... 374
Description ... 374
CLI ... 375
Procedure ... 376
URL Block Feature ... 379
Description ... 379

CLI ... 379
Procedure ... 380
Deploying a Security Group in Monitor Mode ... 383
Introduction to Monitor Mode ... 383
Example Topology for Monitor Mode ... 384
Supported Software Blades in Monitor Mode ... 385
Limitations in Monitor Mode ... 387
Configuring a Security Group in Gateway mode in Monitor Mode ... 388
Configuring a Security Group in VSX mode in Monitor Mode ... 400
Configuring Specific Software Blades for Monitor Mode ... 411
Configuring the Threat Prevention Software Blades for Monitor Mode ... 412
Configuring the Application Control and URL Filtering Software Blades for Monitor Mode ... 414
Configuring the Data Loss Prevention Software Blade for Monitor Mode ... 415
Configuring the Security Group in Monitor Mode Behind a Proxy Server ... 417
Deploying a Security Group in Bridge Mode ... 418
Introduction to Bridge Mode ... 418
Example Topology for Bridge Mode ... 419
Supported Software Blades in Bridge Mode ... 420
Limitations in Bridge Mode ... 422
Configuring a Security Group in Bridge Mode ... 423
Accept, or Drop Ethernet Frames with Specific Protocols ... 432
Routing and Bridge Interfaces ... 434
IPv6 Neighbor Discovery ... 435
Managing Ethernet Protocols ... 436
Troubleshooting ... 438
Collecting System Information (asg_info) ... 438
Description ... 438
Granularity of Commands ... 439
Collected Files ... 439

Syntax and Parameters ... 440
Configuration Files ... 443
General Diagnostic in Security Groups ... 444
Configuration Verifiers ... 447
MAC Verification (mac_verifier) ... 447
Layer 2 Bridge Verifier (asg_br_verifier, asg_brs_verifier) ... 449
Verifying VSX Gateway Configuration (asg vsx_verify) ... 451
Log and Configuration Files ... 454
Installing the Gaia Operating System on a Quantum Maestro Orchestrator ... 457
Reset an Orchestrator to Factory Defaults ... 457
Clean Install of the Gaia Image on an Orchestrator with a Bootable USB Device ... 458
Replacing a Quantum Maestro Orchestrator ... 459
Glossary ... ***460***

Introduction

Quantum Maestro Orchestrator is a scalable Network Security System built to secure the largest networks in the world by orchestrating multiple Check Point Security Appliances into a unified system.

The Quantum Maestro Orchestrator provides:

- Security of infinite scale
- Redundancy - Quantum Maestro Orchestrator automatically distributes traffic between the Security Appliances assigned to Security Groups
- Ability to connect more Security Appliances and use their resources easily in the existing Security Groups

Important Links

For more about Maestro and to download the software, see the Maestro R80.20SP Home Page: sk138233.

- Read the Scalable Platforms Known Limitations in sk148074.
- Read the R80.20 Known Limitations in sk122486.
- To learn about the differences between R80.20 and R80.20SP versions, see sk147033.

  To learn about the differences between different Scalable Platform versions, see sk173183.

Visit the *Check Point CheckMates Community*:

- Start discussions.
- Get answers from experts.
- Join the API community to get code samples and share yours

Security Group Concepts

This section describes some of the Security Group concepts.

Single Management Object (SMO) and Policies

In This Section:

Single Management Object 19
Installing and Uninstalling Policies 22
Working with Policies (asg policy) 23

Single Management Object

Single Management Object (SMO) is a Check Point technology that manages the Security Group as one large Security Gateway with one management IP address.

One Security Group Member, the SMO Master, handles all management tasks, such as Security Gateway configuration, policy installation, remote connections, and logging

are handled. The SMO Master updates all other Security Group Members.

The Active Security Group Member with the lowest ID number is automatically assigned to be the SMO.

Use the "`asg stat -i tasks`" command to identify the SMO and see how tasks are distributed on the Security Group Members (see *"Showing Hardware State (asg stat)" on page 264*).

Example output in a Dual Site configuration

The SMO task runs on Site #2 - on the Security Group Member #3, on which you ran this command (see the string "`(local)`").

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |                            |         3(local)           |
| General (1)        |         2                  |         3(local)           |
| LACP (2)           |         2                  |         3(local)           |
| CH Monitor (3)     |         2                  |         3(local)           |
| DR Manager (4)     |                            |         3(local)           |
| UIPC (5)           |         2                  |         3(local)           |
| Alert (6)          |                            |         3(local)           |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
[Expert@MyChassis-ch0x-0x:0]# member 2_4
Moving to member 2_4
... ...
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |                            |         3                  |
| General (1)        |         2                  |         3                  |
| LACP (2)           |         2                  |         3                  |
| CH Monitor (3)     |         2                  |         3                  |
| DR Manager (4)     |                            |         3                  |
| UIPC (5)           |         2                  |         3                  |
| Alert (6)          |                            |         3                  |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example output from all Security Group Members (in our example, there are two on each Site):

```
[Expert@MyChassis-ch0x-0x:0]# g_all asg stat -i tasks
1_01:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1(local)           |                            |
| General (1)        |         1(local)           |         1                  |
| LACP (2)           |         1(local)           |         1                  |
| CH Monitor (3)     |         1(local)           |         1                  |
| DR Manager (4)     |         1(local)           |                            |
| UIPC (5)           |         1(local)           |         1                  |
| Alert (6)          |         1(local)           |                            |
-------------------------------------------------------------------------------

1_02:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1                  |
| LACP (2)           |         1                  |         1                  |
| CH Monitor (3)     |         1                  |         1                  |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1                  |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------

2_01:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1(local)           |
| LACP (2)           |         1                  |         1(local)           |
| CH Monitor (3)     |         1                  |         1(local)           |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1(local)           |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------

2_02:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1                  |
| LACP (2)           |         1                  |         1                  |
| CH Monitor (3)     |         1                  |         1                  |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1                  |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example output in a Single Site configuration

The SMO task runs on the Security Group Member #1, on which you ran this command (see the string "`(local)`").

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)    |                       Chassis 1                         |
-------------------------------------------------------------------------------
| SMO (0)           |                        1(local)                         |
| General (1)       |                        1(local)                         |
| LACP (2)          |                        1(local)                         |
| CH Monitor (3)    |                        1(local)                         |
| DR Manager (4)    |                        1(local)                         |
| UIPC (5)          |                        1(local)                         |
| Alert (6)         |                        1(local)                         |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Installing and Uninstalling Policies

Installing a Policy

To install a policy on the Security Group, click **Install Policy** in SmartConsole.

The policy installation process includes these steps:

1. The Management Server installs the policy on the SMO Master.
2. The SMO Master copies the policy to all Security Group Members in the Security Group.
3. Each Security Group Member in the Security Group installs the policy locally.

During the policy installation, each Security Group Member sends and receives policy status updates to and from the other Security Group Members in the Security Group. This is because the Security Group Members must install their policies in a synchronized manner.

Note - When you create a Security Group, its Security Group Members enforce an initial policy that allows only the implied rules necessary for management.

Uninstalling a Policy

Note - You cannot uninstall policies from a Security Group in SmartConsole.

Step	Instructions
1	Connect over a serial port to the SMO in the Security Group.
2	Log in to the Gaia gClish.
3	Uninstall the policy: `asg policy unload` See *"Working with Policies (asg policy)" on the next page*.

Working with Policies (asg policy)

Description

Use the "`asg policy`" command in Gaia gClish or the Expert mode to perform policy-related actions.

Syntax

`asg policy -h`
`asg policy {verify | verify_amw} [-vs <VS IDs>] [-a] [-v]`
`asg policy unload [--disable_pnotes] [-a]`
`asg policy unload --ip_forward`

Best Practice - Run these commands over a serial connection to Security Group Members in the Security Group.

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`verify`	Confirms that the correct policies are installed on all Security Group Members in the Security Group.
`verify_amw`	Confirms that the correct Anti-Malware policies are installed on all Security Group Members in the Security Group.
`unload`	Uninstalls the policy from all Security Group Members in the Security Group.
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.
`-v`	Shows detailed verification results for Security Group Members.
`-a`	Runs the verification on Security Group Members in both UP and DOWN states.
`--disable_pnotes`	Security Group Members stay in the UP state without an installed policy. **Important** - If you omit this option, Security Group Members go into the DOWN state until the policy is installed again!
`--ip_forward`	Enables IP forwarding.

Examples

Example 1 - Detailed verification results for Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# asg policy verify -v
+-------------------------------------------------------------------------+
|Policy Verification                                                      |
+-------+------------------+---------------+-----------------+---------+
|SGM    |Policy Name       |Policy Date    |Policy Signature |Status   |
+-------+------------------+---------------+-----------------+---------+
|1_01   |Standard          |27Feb19 08:56  |e17c177f7        |Success  |
+-------+------------------+---------------+-----------------+---------+

+-------------------------------------------------------------------------------+
|Summary                                                                        |
+-------------------------------------------------------------------------------+
|Policy Verification completed successfully                                     |
+-------------------------------------------------------------------------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2 - Detailed verification results for for each Virtual System on Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# asg policy verify -vs all -v
+-------------------------------------------------------------------------------+
|Policy Verification                                    |                       |
+-------+-------+------------------+---------------+-----------------+---------+
|VS     |SGM    |Policy Name       |Policy Date    |Policy Signature |Status   |
+-------+-------+------------------+---------------+-----------------+---------+
|0      |1_01   |Standard          |27Feb19 08:56  |996eee5e6        |Success  |
|       |1_03   |Standard          |27Feb19 08:56  |996eee5e6        |Success  |
|       |1_04   |Standard          |27Feb19 08:56  |996eee5e6        |Success  |
|       |1_05   |Standard          |27Feb19 08:56  |996eee5e6        |Success  |
|       |1_06   |Standard          |27Feb19 08:56  |996eee5e6        |Success  |
|       |1_11   |Standard          |27Feb19 08:56  |996eee5e6        |Success  |
|       |1_12   |Standard          |27Feb19 08:56  |996eee5e6        |Success  |
+-------+-------+------------------+---------------+-----------------+---------+
|1      |1_01   |Standard          |27Nov12 13:03  |836fa2ec1        |Success  |
|       |1_03   |Standard          |27Nov12 13:03  |836fa2ec1        |Success  |
|       |1_04   |Standard          |27Nov12 13:03  |836fa2ec1        |Success  |
|       |1_05   |Standard          |27Nov12 13:03  |836fa2ec1        |Success  |
|       |1_06   |Standard          |27Nov12 13:03  |836fa2ec1        |Success  |
|       |1_11   |Standard          |27Nov12 13:03  |836fa2ec1        |Success  |
|       |1_12   |Standard          |27Nov12 13:03  |836fa2ec1        |Success  |
+-------+-------+------------------+---------------+-----------------+---------+
|2      |1_01   |Standard          |27Feb19 08:56  |10eef9ced        |Success  |
|       |1_03   |Standard          |27Feb19 08:56  |10eef9ced        |Success  |
|       |1_04   |Standard          |27Feb19 08:56  |10eef9ced        |Success  |
|       |1_05   |Standard          |27Feb19 08:56  |10eef9ced        |Success  |
|       |1_06   |Standard          |27Feb19 08:56  |10eef9ced        |Success  |
|       |1_11   |Standard          |27Feb19 08:56  |10eef9ced        |Success  |
|       |1_12   |Standard          |27Feb19 08:56  |10eef9ced        |Success  |
+-------+-------+------------------+---------------+-----------------+---------+

+-------------------------------------------------------------------------------+
|Summary                                                                        |
+-------------------------------------------------------------------------------+
|Policy Verification completed successfully                                     |
+-------------------------------------------------------------------------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Example 3 - Uninstall of a Policy

```
[Expert@MyChassis-ch0x-0x:0]# asg policy unload
You are about to perform unload policy on blades: all
All SGMs will be in DOWN state, beside local SGM. It is recommended to run the procedure
via serial connection

Are you sure? (Y - yes, any other key - no) y

Unload policy requires auditing
Enter your full name: John Doe
Enter reason for unload policy [Maintenance]:
WARNING: Unload policy on blades: all, User: John Doe, Reason: Maintenance
+--------------------------------+
|Unload policy                   |
+---------------+----------------+
|SGM            |Status          |
+---------------+----------------+
|1_3            |Success         |
+---------------+----------------+
|1_2            |Success         |
+---------------+----------------+
|1_1            |Success         |
+---------------+----------------+
|2_3            |Success         |
+---------------+----------------+
|2_2            |Success         |
+---------------+----------------+
|2_1            |Success         |
+---------------+----------------+

+-------------------------------------------------------------------------------+
|Summary                                                                        |
+-------------------------------------------------------------------------------+
|Unload policy completed successfully                                           |
+-------------------------------------------------------------------------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Policy Management on Security Group Members

In This Section:

Synchronizing Policy and Configuration Between Security Group Members 28
Understanding the Configuration File List 29
MAC Addresses and Bit Conventions 31
MAC Address Resolver (asg_mac_resolver) 34

Because the Security Group works as one large Security Gateway, all Security Group Members are configured with the same policy.

When you install a policy from the Management Server, it first installs the policy on the SMO Security Group Member.

The SMO copies the policy and Security Group Member configuration to all Security Group Members in the UP state.

When the Security Group Member enters the UP state, it automatically gets the installed policy and configurations that are installed, from the SMO.

When there is only one Security Group Member in the UP state, it is possible there is no SMO. Then, that Security Group Member uses its local policy and configuration.

If there are problems with the policy or configuration on the Security Group Member, you can manually copy the information from a different Security Group Member.

The Security Group Member configuration has these components:

- Firewall policy, which includes the Rule Base.
- Set of configuration files defined in the `/etc/xfer_file_list` file.

  This file contains the location of all related configuration files.

  It also defines the action to take if the copied file is different from the one on the local Security Group Member.

Synchronizing Policy and Configuration Between Security Group Members

Use the "`asg_blade_config pull_config`" command in Gaia gClish to synchronize the policies manually.

Optionally, it can configure files from a specified source Security Group Member to the target Security Group Member.

The target Security Group Member is the Security Group Member you use to run this command.

To synchronize Security Group Members manually:

Step	Instructions
1	Run: `> asg_blade_config pull_config`

2	Do **one** of these:
	■ Reboot the **target**Security Group Member:
	`reboot -b <Security Group Member ID>`
	■ Start the Check Point services and remove the ClusterXL Critical Device "`admin_down`":
	`cpstart`
	`clusterXL_admin up`

Note - You can run the "`asg stat -i all_sync_ips`" command in Gaia gClish to get a list of all synchronization IP addresses on the Security Group Member.

Understanding the Configuration File List

The `/etc/xfer_file_list` file contains pointers to the related configuration files on the Security Group Member. Each record defines the path to a configuration file, followed by the action to take if the imported file is different from the local file. This table shows an example of the record structure.

Context	File name and path	Action
`global_context`	`$FWDIR/boot/modules/fwkern.conf`	`/bin/false`

The context field defines the type of configuration file:

- `global_context` - Security Gateway configuration file
- `all_vs_context` - Virtual Systems configuration file

The action field defines the action to take when the imported (copied) file is different than the local file:

- `/bin/true` - Reboot is **not** required
- `/bin/false` - Reboot **is** required
- String enclosed in double quotes - Name of a "callback script" that selects the applicable action.

Example - Configuration file list

```
[Expert@MyChassis-ch0x-0x:0]# g_cat /etc/xfer_file_list
#The Columns are:
#1) global_context or all_vs_context - VSX support.
#       It separates the files relevant to all VSs (all_vs_context) from those which are only
relevant for VS0 (global_context)
#       In a security gateway mode, there is no difference between the two values
#2) File location in the SMO - where to pull the files from
#3) Action to perform after the file is copied, if it's different.
#       The result of the operation determines if a reboot is needed after the operation - 1
for reboot, 0 for no reboot
#       Please Notice - /bin/false => reboot, /bin/true => don't reboot
#4) [Optional] A local path to copy the file to, needed if different from the source

global_context /opt/CPda/bin/policy.xml /bin/true
global_context /etc/upgrade_pkg-0.1-cp989000001.i386.rpm "rpm -U --force --nodeps
/etc/upgrade_pkg-0.1-cp989000001.i386.rpm"
global_context /etc/sysconfig/image.md5 "/usr/lib/smo/libclone.tcl --clone --rsip --xfer --
reboot"
global_context $PPKDIR/boot/modules/sim_aff.conf "sim affinityload"
global_context $PPKDIR/boot/modules/simkern.conf /bin/false
global_context $FWDIR/boot/boot.conf /bin/false
global_context $FWDIR/boot/modules/fwkern.conf /bin/false
all_vs_context $FWDIR/conf/fwauthd.conf /bin/false
all_vs_context $FWDIR/conf/discntd.if /bin/false
#global_context /var/opt/fw.boot/ha_boot.conf /bin/false
global_context /config/active  /usr/bin/confd_clone /config/db/cloned_db
global_context /tmp/sms_rate_limit.tmp /bin/true
global_context /tmp/sms_history.tmp /bin/true
global_context /home/admin/.ssh/known_hosts /bin/true
global_context /etc/passwd /bin/true
global_context /etc/shadow /bin/true
... output is cut for brevity ...
global_context /etc/smodb.json  "/usr/lib/smo/libclone_smodb.tcl clone_smodb_apply"
/tmp/smo_smodb.json
global_context $FWDIR/conf/prioq.conf   /bin/false
global_context /web/templates/httpd-ssl.conf.templ /usr/scripts/generate_httpd-ssl_conf.sh
all_vs_context $FWDIR/conf/fwaccel_dos_rate_on_install /bin/false
all_vs_context $FWDIR/conf/fwaccel6_dos_rate_on_install /bin/false
global_context $FWDIR/database/sam_policy.db $SMODIR/scripts/compare_samp_db.tcl /tmp/sam_
policy.db.new
global_context $FWDIR/database/sam_policy.mng /bin/false
all_vs_context $FWDIR/conf/icap_client_blade_configuration.C /bin/true
global_context $CPDIR/conf/chassis_priority_db.C /bin/true
[Expert@MyChassis-ch0x-0x:0]#
```

MAC Addresses and Bit Conventions

MAC addresses on the system are divided into these types - BMAC, VMAC, and SMAC:

BMAC

A MAC address assigned to all interfaces with the naming convention "`BPEthX`".

This is unique for each Security Group Member.

It does not rely on the interface index number.

Bit convention for the BMAC type:

Bit range	Instructions
1	Distinguishes between VMAC and other MAC addresses. This is used to prevent possible collisions with VMAC space. Possible values are: ■ `0` - BMAC or SMAC ■ `1` - VMAC
2-8	Security Group Member ID (starting from 1). This is limited to 127.
9-13	Always zero.
14	Distinguishes between BMAC and SMAC addresses. This is used to prevent possible collisions with SMAC space. Possible values: ■ `0` - BMAC ■ `1` - SMAC
15-16	Absolute interface number. This is taken from the interface name. When the `BPEthX` format is used, `X` is the interface number. This is limited to four interfaces.

VMAC

A MAC address assigned to all interfaces with the naming convention "`eth`*`X`*`-`*`YZ`*".

This is unique for each Site.

It does not rely on the interface index number.

Bit convention for the VMAC type:

Bit range	Instructions
1	Distinguishes between VMAC and other MAC addresses. This is used to prevent possible collisions with VMAC space. Possible values are: ■ `0` - BMAC or SMAC ■ `1` - VMAC
2-3	Site ID. Limited to 2 Sites.
4-8	Switch number. Limited to 32 switches.
9-16	Port number. Limited to 256 for each switch.

SMAC

A MAC address assigned to Sync interfaces.

This is unique for each Security Group Member.

It does not rely on the interface index number.

Bit convention for the SMAC type:

Bit range	Instructions
1	Distinguishes between VMAC and other MAC addresses. This is used to prevent possible collisions with VMAC space. Possible values are: ■ `0` - BMAC or SMAC ■ `1` - VMAC
2-8	Security Group Member ID (starting from 1). This is limited to 127.
9-13	Always zero.
14	Distinguishes between BMAC and SMAC addresses. This is used to prevent possible collisions with SMAC space. Possible values: ■ `0` - BMAC ■ `1` - SMAC
15	Always zero.
16	Sync interface. Possible values are: ■ `0` - Sync1 ■ `1` - Sync2

MAC Address Resolver (asg_mac_resolver)

Description

Use the "`asg_mac_resolver`" command in Gaia gClish or the Expert mode to make sure that all types of MAC addresses (BMAC, VMAC, and SMAC) are correct.

From the MAC address you provide, the "`asg_mac_resolver`" command determines the:

- MAC type
- Site ID
- Security Group Member ID
- Assigned interface

Syntax

```
asg_mac_resolver <MAC address>
```

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_mac_resolver 00:1C:7F:01:00:FE
[00:1C:7F:01:00:FE, BMAC] [Chassis ID: 1] [SGM ID: 1] [Interface: BPEth0]
[Expert@MyChassis-ch0x-0x:0]#
```

Notes:

- The specified MAC Address comes from BPEth0 on Security Group Member #1 on the Site #1.
- `00:1C:7F:01:00:FE` is the Magic MAC attribute, which is identified by "`FE`".
- The index length is 16 bits (2 Bytes) identified by 01:00 x x x x x x x x x x x x x x x x.

Configuring Security Groups

This section provides a workflow and step-by-step instructions for configuring Security Groups.

Workflow

Note - It is assumed that you already installed the Quantum Maestro Orchestrators, the Security Appliances, and connected all cables. See the *Quantum Maestro Getting Started Guide*.

1. **Change the default Gaia password to a new password on the Quantum Maestro Orchestrators**

   On the Quantum Maestro Orchestrators, change the default Gaia password from "`admin`" to a new password.

Step	Instructions
a	With a web browser, connect to the Gaia Portal of the Quantum Maestro Orchestrator: `https://<IP Address of MGMT Port on Quantum Maestro Orchestrator>`
b	Log in with these default credentials: ▪ Username - `admin` ▪ Password - `admin`
c	From the left tree, click **User Management > Users**.
d	Select the **admin** user.
e	Click **Reset Password**.
f	Enter the new password.
g	Click **OK**.

2. **Configure the applicable Security Groups on the Quantum Maestro Orchestrators**

   Note - Configure only one of the installed Quantum Maestro Orchestrators. The Quantum Maestro Orchestrators synchronize the configuration automatically with each other.

   Every Security Group must contain:

a. One or more Security Appliances.

Note - The Quantum Maestro Orchestrators automatically assign the corresponding Downlink ports.

b. Applicable ports on the Quantum Maestro Orchestrators:

- A dedicated port, which connects the Security Group to the Management Server.
- Uplink ports, to which you connected the external traffic and internal traffic networks.

You can configure Security Groups in:

- Gaia Portal (see *"Configuring Security Groups in Gaia Portal" on page 44*).
- Gaia Clish (see *"Configuring Security Groups in Gaia Clish" on page 56*).

In addition, see *"Summary of Configuration Options" on page 40*.

Perform these steps:

Step	Instructions
a	Create a new Security Group.
b	Add the Network Configuration to the Security Group.
c	Configure the First Time Wizard settings in the Security Group. **Note** - This First Time Wizard configures only a limited number of settings.
d	Assign the available Security Appliances to the Security Group. **Important:** ▪ You can assign only Security Appliances of the same model to the same Security Group. ▪ Security Appliances assigned to the Security Group automatically reboot after you apply the configuration. **Best Practice for Dual Site** - Assign the same number (as possible) of Security Appliances from each site to the Security Group. If a failover occurs between the sites, Security Appliances on the new Active site must be able to process all the traffic.
e	Assign the applicable Quantum Maestro Orchestrator ports to the Security Group (Uplink ports and a Management interface).

3. **Configure the Gaia Operating System settings in the new Security Group**

See *"Configuring Gaia Settings of a Security Group" on page 91*.

4. **Configure the settings in SmartConsole**

   See *"Configuration in SmartConsole" on page 93*.

   - For a Security Group in **Gateway** mode:
     a. Create one Security Gateway object.
     b. Configure the applicable Security Policy.
     c. Install the Security Policy on the Security Gateway object.
   - For a Security Group in **VSX** mode:
     a. Create one VSX Gateway object.
     b. Create the objects of Virtual Systems.
     c. Configure the applicable Security Policies for the Virtual Systems.
     d. Install the Security Policies on the Virtual Systems.

5. **Make sure the traffic passes as expected**

   Initiate connections that must pass through this Security Group.

Best Practice - Create a Gaia Backup on the Quantum Maestro Orchestrators to save the configuration. For more information, see the *R80.20SP Quantum Maestro Gaia Administration Guide* > Chapter *Maintenance* > Section *System Backup*.

Configuration Procedure

You can configure Security Groups on Quantum Maestro Orchestrators:

- In Gaia Portal (see *"Configuring Security Groups in Gaia Portal" on page 44*)
- In Gaia Clish (see *"Configuring Security Groups in Gaia Clish" on page 56*)

In addition, see *"Summary of Configuration Options" on page 40*.

Workflow for Configuring Security Groups

You can configure the Security Groups in Gaia Portal (see *"Configuring Security Groups in Gaia Portal" on page 44*), or Gaia Clish (see *"Configuring Security Groups in Gaia Clish" on page 56*).

In addition, see *"Summary of Configuration Options" on page 40*.

Step	Instructions
1	Create a new Security Group. **Note** - Configure only one of the installed Quantum Maestro Orchestrators. The Quantum Maestro Orchestrators synchronize the configuration automatically with each other. **Best Practice** - Configure the **First Time Wizard settings** in the new Security Group.
2	Assign the applicable Security Appliances to the Security Group. **Important:** ■ You can assign only Security Appliances of the same model to the same Security Group. ■ Security Appliances assigned to the Security Group automatically reboot after you apply the configuration. **Best Practice for Dual Site** - Assign the same number (as possible) of Security Appliances from each site to the Security Group. If a failover occurs between the sites, Security Appliances on the new Active site must be able to process all the traffic.
3	Assign the applicable Quantum Maestro Orchestrator ports to the Security Group (Uplink ports and a Management interface).
4	Verify and apply the configuration.

Step	Instructions
5	If you did not configure the **First Time Wizard settings** when you created a Security Group, you must run the Gaia First Time Configuration Wizard on every Security Appliance in the Security Group. 1. With a web browser, connect to the Gaia Portal of the Security Group: `https://<IP Address of Security Group>` **Important** - This connection goes through the Quantum Maestro Orchestrator's management interface you assigned to this Security Group. 2. The Gaia First Time Configuration Wizard starts. Follow the instructions on the screen.

Summary of Configuration Options

Table: Summary of configuration options in Quantum Maestro Orchestrators

Configuration Option	In Gaia Portal	In Gaia Clish *
Configuring the number of Maestro sites (Single Site or Dual Site)	N / A	See *"Configuring the Number of Maestro Sites" on page 59*
Viewing the configured number of Maestro sites	1. Click **Orchestrator** page. 2. In the **Topology** pane, open the Security Groups.	See *"Viewing the Number of Maestro Sites" on page 60*
Configuring the Site ID in the Dual Site deployment	N / A	See *"Configuring the Site ID in Dual Site Deployment" on page 60*
Viewing the Site ID in the Dual Site deployment	N / A	See *"Viewing the Site ID in Dual Site Deployment" on page 60*
Creating a New Security Group	See *"Creating a New Security Group" on page 45*	See *"Creating a New Security Group" on page 61*
Deleting a Security Group	See *"Deleting a Security Group" on page 46*	See *"Creating a New Security Group" on page 61*
Adding the Network Configuration to a Security Group	See *"Adding the Network Configuration and First Time Wizard settings to a Security Group" on page 47*	See *"Adding the Network Configuration to a Security Group" on page 63*
Removing the Network Configuration from a Security Group	See *"Removing the Network Configuration and First Time Wizard settings from a Security Group" on page 48*	See *"Removing the Network Configuration from a Security Group" on page 64*
Configuring the First Time Wizard settings in a Security Group	See *"Adding the Network Configuration and First Time Wizard settings to a Security Group" on page 47*	See *"Configuring First Time Wizard settings in a Security Group" on page 65*

Table: Summary of configuration options in Quantum Maestro Orchestrators (continued)

Configuration Option	In Gaia Portal	In Gaia Clish *
Removing the First Time Wizard settings from a Security Group	See *"Removing the Network Configuration and First Time Wizard settings from a Security Group" on page 48*	See *"Removing First Time Wizard settings from a Security Group" on page 66*
Assigning available Security Appliances to a Security Group	See *"Assigning Available Security Appliances to a Security Group" on page 49*	See *"Assigning One Security Appliance to a Security Group" on page 67*
Removing one Security Appliance from a Security Group	See *"Removing One Security Appliance from a Security Group" on page 50*	See *"Removing One Security Appliance from a Security Group" on page 69*
Removing all Security Appliances from a Security Group	See *"Removing All Security Appliances from a Security Group" on page 50*	N / A
Moving Security Appliances from one Security Group to a different Security Group	See *"Moving Security Appliances from One Security Group to a Different Security Group" on page 51*	N / A
Assigning Interfaces to a Security Group	See *"Assigning Interfaces to a Security Group" on page 52*	See *"Assigning One Interface to a Security Group" on page 71*
Removing one interface from a Security Group	See *"Removing One Interface from a Security Group" on page 52*	See *"Removing One Interface from a Security Group" on page 72*
Removing all interfaces from a Security Group	See *"Removing All Interfaces from a Security Group" on page 53*	N / A
Moving interfaces from one Security Group to a different Security Group	See *"Moving Interfaces from One Security Group to a Different Security Group" on page 53*	N / A
Adding VLAN interfaces on Uplink ports	See *"Adding VLAN Interfaces on Uplink Ports" on page 54* See *"Configuring VLAN Interfaces on Uplink Ports" on page 124*	See *"Adding VLAN Interfaces on Uplink Ports" on page 73* See *"Configuring VLAN Interfaces on Uplink Ports" on page 124*

Table: Summary of configuration options in Quantum Maestro Orchestrators (continued)

Configuration Option	In Gaia Portal	In Gaia Clish *
Viewing VLAN interfaces on Uplink ports	See *"Configuring VLAN Interfaces on Uplink Ports" on page 124* Follow these steps: 1. Click **Orchestrator** page. 2. See the **Unassigned Interfaces** column. or these steps: 1. Click **Orchestrator** page. 2. Click the **[+]** on the left side of the applicable Security Group. 3. Click the **[+]** on the left side of the **Interfaces** section.	See *"Viewing VLAN Interfaces on Uplink Ports" on page 74* See *"Configuring VLAN Interfaces on Uplink Ports" on page 124*
Removing VLAN interfaces from Uplink ports	See *"Removing VLAN Interfaces from Uplink Ports" on page 55*	See *"Removing VLAN Interfaces from Uplink Ports" on page 76*
Verifying the configuration changes in Security Groups	Automatic	See *"Verifying the Configuration Changes" on page 77*
Applying the configuration changes to Security Groups	In the bottom left corner, click **Apply**.	See *"Applying the Configuration Changes" on page 78*
Deleting configuration changes in Security Groups that were not applied yet	In the bottom left corner, click **Refresh**.	See *"Deleting Configuration Changes That Were Not Applied Yet" on page 79*
Configuring the port settings	N / A	See *"Configuring the Port Settings" on page 80*
Viewing the port settings	N / A	See *"Viewing the Port Settings" on page 86*

Table: Summary of configuration options in Quantum Maestro Orchestrators (continued)

Configuration Option	In Gaia Portal	In Gaia Clish *
Viewing the Security Group settings	1. Click **Orchestrator** page. 2. In the **Topology** column, click the **[+]** on the left side of the **Security Groups**. 3. Click the **[+]** on the left side of the applicable Security Group.	See *"Viewing the Security Group Settings" on page 90*

*Important - After every change in Gaia Clish, verify (see *"Verifying the Configuration Changes" on page 77*) and then apply (see *"Applying the Configuration Changes" on page 78*) the new configuration.

Configuring Security Groups in Gaia Portal

To start working in Gaia Portal:

Step	Instructions
1	With a web browser, connect to the Gaia Portal on the Quantum Maestro Orchestrator: `https://<IP Address of Orchestrator's MGMT Port>`
2	Log in to the Gaia Portal with these default credentials: ■ Username - `admin` ■ Password - `admin`
3	From the left navigation tree, click **Orchestrator** page.

The **Topology** section contains the table that shows:

Item	Description
Unassigned Gateways	All detected Security Appliances that are not part of configured Security Groups. Quantum Maestro Orchestrator listens on the ports and automatically detects the connected Security Appliances.
Topology	Configured Security Groups with their assigned Security Appliances and ports.
Unassigned Interfaces	All interfaces on Quantum Maestro Orchestrators that are not part of configured Security Groups.

Notes:

- Click **Apply** button to save the changes in Security Groups.
- Click **Refresh** button to load the latest configuration. For example, when you work with two Quantum Maestro Orchestrators for redundancy, and you change the configuration on another Quantum Maestro Orchestrator.
- You use the drag-and-drop action on the Security Appliance and port objects.
- When you hover the mouse cursor over a Security Appliance object, the tooltip shows the Security Appliance ID in the Security Group, Appliance Serial Number and the corresponding Downlink port.

Applicable configuration procedures are provided below.

Creating a New Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	In the **Topology** column, right-click on the **Security Groups** and select **New Security Group**.
3	Enter the required **Management interface settings**. **Best Practice** - Configure the **First Time Wizard settings**.
4	Click **OK**.
5	Click the **[+]** on the left side of the **Security Groups** and the new Security Group.
6	In the **Unassigned Gateways** column, select the applicable Security Appliances. **Important** - You must assign at least one Security Appliance to the Security Group. **Note** - To select multiple Security Appliances, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
7	Drag-and-drop the selected Security Appliances from the **Unassigned Gateways** column to the **Gateways** section in the new Security Group.
8	In the **Unassigned Interfaces** column, select the applicable data and management interfaces. **Note** - To select multiple interfaces, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
9	Drag-and-drop the selected interfaces from the **Unassigned Interfaces** column to the **Interfaces** section in the new Security Group.
10	In the bottom left corner, click **Apply**.

Notes:

- Every new Security Group you add, is called **Security Group N**, where the ordinal number *N* is assigned automatically starting from 1 (for example, if you already have "Security Group 1" and "Security Group 3", then the new Security Group is called "Security Group 2").
- Every Security Group contains two sections:
  - **Gateways** - contains the Check Point Security Gateways you assign to this Security Group.
  - **Interfaces** - contains the Orchestrator's interfaces you assign to this Security Group.
- You must make sure to assign the correct Security Gateways' interfaces to Security Groups.

Deleting a Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	In the **Topology** column, right-click on the Security Group.
3	From the menu, click **Delete Security Group**. **Important** - There is no prompt to confirm.
4	In the bottom left corner, click **Apply**.

Adding the Network Configuration and First Time Wizard settings to a Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	In the **Topology** column, right-click on the Security Group.
3	Click **Set Security Group configuration**.
4	In the **Network settings** section: 1. In the **IPv4 address** field, enter the IPv4 address of the Security Group. All Security Appliances in this Security Group use this IPv4 address as their Gaia management IP address. You use this IPv4 address in SmartConsole when you configure the corresponding Security Gateway object. 2. In the **Subnet mask** field, enter the applicable IPv4 subnet mask. All Security Appliances in this Security Group use this IPv4 subnet mask for their Gaia management IP address. You use this IPv4 subnet mask in SmartConsole when you configure the corresponding Security Gateway object. 3. In the **Default Gateway** field, enter the applicable IPv4 address. All Security Appliances in this Security Group use this IPv4 address as their default gateway.
5	In the **First Time Wizard settings** section, configure the initial settings for Security Appliances assigned to this Security Group. 1. Select **Set FTW configuration**. 2. In the **Host Name** field, enter a hostname. 3. In the **Activation Key** field, enter a one-time activation key (between 4 and 127 characters long). 4. In the **Confirm Activation Key** field, enter the same one-time activation key again. 5. Select **Install as VSX**, only if it is necessary to run all Security Appliances in this Security Group as VSX Gateways.
6	Click **OK**.
7	In the bottom left corner, click **Apply**.

Warning - If you enable the **Set FTW configuration** option in an existing Security Group (in which you already ran the First Time Configuration Wizard), then the change applies only after you reset each Security Appliance in that Security Group to factory defaults.

Removing the Network Configuration and First Time Wizard settings from a Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	In the **Topology** column, right-click on the Security Group.
3	From the menu, click **Clear network configuration**. **Important** - There is no prompt to confirm.
4	In the bottom left corner, click **Apply**.

Note - This configuration option is available only in the Gaia Portal.

Assigning Available Security Appliances to a Security Group

Best Practice:

1. Before you add Security Appliances to an existing Security Group, enable the SMO Image Cloning feature in the Security Group.
   This feature automatically clones all the required software packages to the new Security Appliances.
   Run in Gaia gClish on the Security Group:

   ```
   set smo image auto-clone state on
   ```

   ```
   show smo image auto-clone state
   ```

2. After you added the Security Appliances, you must disable the SMO Image Cloning feature in the Security Group:

   ```
   set smo image auto-clone state off
   ```

   ```
   show smo image auto-clone state
   ```

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable Security Group.
3	In the **Unassigned Gateways** column, select the applicable Security Appliances. **Note** - To select multiple Security Appliances, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
4	Drag-and-drop the selected Security Appliances from the **Unassigned Gateways** column to the **Gateways** section in the applicable Security Group. **Note** - If such operation is allowed, Gaia Portal shows a green plus icon. Otherwise, it shows a red blocking icon.
5	In the bottom left corner, click **Apply**.

Important:

- You can assign only appliances of the same model to the same Security Group.
- The Security Appliances must reboot after you assign them to a Security Group.

Best Practice for Dual Site - Assign the same number (as possible) of Security Appliances from each site to the Security Group. If a failover occurs between the sites, Security Appliances on the new Active site must be able to process all the traffic.

Removing One Security Appliance from a Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable Security Group.
3	Click the **[+]** on the left side of the **Gateways** section.
4	Select the Security Appliance it is necessary to remove from the Security Group.
5	Right-click on the selected Security Appliance.
6	From the menu, click **Detach Gateway**. **Important** - There is no prompt to confirm.
7	In the bottom left corner, click **Apply**.

Important - The Security Appliance must perform a reset to factory defaults and reboot after you remove it from a Security Group. This is to make sure that no security configuration is left behind.

Removing All Security Appliances from a Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable Security Group.
3	Left-click on the **Gateways** section to select it.
4	Right-click on the **Gateways** section.
5	From the menu, click **Detach all Gateways**.
6	In the bottom left corner, click **Apply**.

Important - The Security Appliances must perform a reset to factory defaults and reboot after you remove them from a Security Group. This is to make sure that no security configuration is left behind.

Note - This configuration option is available only in the Gaia Portal.

Moving Security Appliances from One Security Group to a Different Security Group

Best Practice:

1. Before you add Security Appliances to an existing Security Group, enable the SMO Image Cloning feature in the Security Group.
   This feature automatically clones all the required software packages to the new Security Appliances.
   Run in Gaia gClish on the Security Group:

   ```
   set smo image auto-clone state on
   show smo image auto-clone state
   ```

2. After you added the Security Appliances, you must disable the SMO Image Cloning feature in the Security Group:

   ```
   set smo image auto-clone state off
   show smo image auto-clone state
   ```

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable *source* Security Group.
3	Click the **[+]** on the left side of the applicable *target* Security Group.
4	Select the applicable Security Appliances. **Note** - To select multiple Security Appliances, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
5	Drag-and-drop the selected Security Appliances from the **Gateways** section of the *source* Security Group to the **Gateways** section of the *target* Security Group. **Note** - If such operation is allowed, Gaia Portal shows a green plus icon. Otherwise, it shows a red blocking icon.
6	In the bottom left corner, click **Apply**.

Important - The Security Appliance must perform a reset to factory defaults and reboot after you remove it from a Security Group. This is to make sure that no security configuration is left behind.

Note - This configuration option is available only in the Gaia Portal.

Assigning Interfaces to a Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable Security Group.
3	In the **Unassigned Interfaces** column, select the applicable interfaces. **Note** - To select multiple interfaces, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
4	Drag-and-drop the selected interfaces from the **Unassigned Interfaces** column to the **Interfaces** section in the applicable Security Group. **Note** - If such operation is allowed, Gaia Portal shows a green plus icon. Otherwise, it shows a red blocking icon.
5	In the bottom left corner, click **Apply**.

Removing One Interface from a Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable Security Group.
3	Click the **[+]** on the left side of the **Interfaces** section.
4	Right-click on the applicable interface.
5	From the menu, click **Detach Interface**. **Important** - There is no prompt to confirm.
6	In the bottom left corner, click **Apply**.

Removing All Interfaces from a Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable Security Group.
3	Right-click on the **Interfaces** section.
4	From the menu, click **Detach Security Group Interfaces**. **Important** - There is no prompt to confirm.
5	In the bottom left corner, click **Apply**.

Note - This configuration option is available only in the Gaia Portal.

Moving Interfaces from One Security Group to a Different Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable *source*Security Group.
3	Click the **[+]** on the left side of the applicable *target*Security Group.
4	Select the applicable interfaces. **Note** - To select multiple interfaces, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
5	Drag-and-drop the selected interfaces from the **Interfaces** section of the *source*Security Group to the **Interfaces** section of the *target*Security Group. **Note** - If such operation is allowed, Gaia Portal shows a green plus icon. Otherwise, it shows a red blocking icon.
6	In the bottom left corner, click **Apply**.

Note - This configuration option is available only in the Gaia Portal.

Adding VLAN Interfaces on Uplink Ports

Important - Starting from the R80.20SP Jumbo Hotfix Accumulator Take 304 on the Quantum Maestro Orchestrator, it is **not** necessary to configure VLAN interfaces on Uplink ports. For more information, see sk170294.

If a Security Group must inspect VLAN traffic, you must configure VLAN interfaces on the applicable Uplink ports.

Step	Instructions
1	**If you did not assign the Uplink port to the Security Group yet:** ▪ In the **Unassigned Interfaces** column, right-click on the Uplink port, on which it is necessary to add a VLAN. **If you already assigned the Uplink port to the Security Group:** 1. In the **Topology** column, click the **[+]** on the left side of the **Security Groups**. 2. Click the **[+]** on the left side of the applicable Security Group. 3. Click the **[+]** on the left side of the Interfaces section. 4. Right-click on the Uplink port, on which it is necessary to add a VLAN.
2	From the menu, click **Add VLAN**.
3	In the **VLAN ID** field, enter or select the VLAN ID between 2 and 4094.
4	In the **Member Of** field, make sure to select the correct Uplink port.
5	Click **OK**.
6	The prompt appears: `In order to create VLAN <ID > for Port <Port ID> (<Interface Name>) it must be removed. Would you like to continue?` Click **Yes**.
7	In the bottom left corner, click **Apply**.

Removing VLAN Interfaces from Uplink Ports

Important - Starting from the R80.20SP Jumbo Hotfix Accumulator Take 304 on the Quantum Maestro Orchestrator, it is **not** necessary to configure VLAN interfaces on Uplink ports. For more information, see sk170294.

Step	Instructions
1	In the **Unassigned Interfaces** column, right-click on the Uplink port with configured VLAN ID it is necessary to remove. **If you did not assign the Uplink port to the Security Group yet:** ▪ In the **Unassigned Interfaces** column, right-click on the Uplink port with configured VLAN ID it is necessary to remove. **If you already assigned the Uplink port to the Security Group:** 1. In the **Topology** column, click the **[+]** on the left side of the **Security Groups**. 2. Click the **[+]** on the left side of the applicable Security Group. 3. Click the **[+]** on the left side of the Interfaces section. 4. Right-click on the Uplink port with configured VLAN ID it is necessary to remove.
2	From the menu, click **Remove VLAN**. **Important** - There is no prompt to confirm.
3	In the bottom left corner, click **Apply**.

Configuring Security Groups in Gaia Clish

This section provides the configuration instructions for Gaia Clish.

Connect to the Command Line on the Quantum Maestro Orchestrator (with SSH, or through the Console Port).

Log in to the Gaia Clish with these default credentials:

- Username - `admin`
- Password - `admin`

These are the main commands in Gaia Clish on Quantum Maestro Orchestrators:

Task	Syntax

Viewing the settings	`show maestro`
	
	Available sub-commands in the '`show maestro`' command
	`[Global] MyChassis-ch01-01 > show maestro [ESC][ESC]`
	`show maestro configuration orchestrator-site-amount`
	`show maestro configuration orchestrator-site-id`
	`show maestro port VALUE admin-state`
	`show maestro port VALUE mtu`
	`show maestro port VALUE optic-info`
	`show maestro port VALUE qsfp-mode`
	`show maestro port VALUE type`
	`show maestro port VALUE vlans`
	`show maestro security-group id VALUE`
	`show maestro security-group verify-new-config`
	`[Global] MyChassis-ch01-01 >`

Task	Syntax

Configuring the settings	`add maestro`
	Available sub-commands in the '`add maestro`' command
	`[Global] MyChassis-ch01-01 > add maestro [ESC][ESC]`
	`add maestro port VALUE vlan VALUE`
	`add maestro security-group id VALUE interface VALUE`
	`add maestro security-group id VALUE serial VALUE`
	`[Global] MyChassis-ch01-01 >`
	`set maestro`
	Available sub-commands in the '`set maestro`' command
	`[Global] MyChassis-ch01-01 > set maestro [ESC][ESC]`
	`set maestro configuration orchestrator-site-amount VALUE`
	`set maestro configuration orchestrator-site-id`
	`set maestro port VALUE admin-state VALUE`
	`set maestro port VALUE mtu VALUE`
	`set maestro port VALUE qsfp-mode VALUE`
	`set maestro port VALUE type VALUE no-confirmation`
	`set maestro security-group apply-new-config`
	`set maestro security-group id VALUE ftw-configuration hostname VALUE sic VALUE is-vsx VALUE`
	`set maestro security-group id VALUE management-connectivity ipv4-address VALUE mask-length VALUE [default-gw VALUE]`
	`[Global] MyChassis-ch01-01 >`

Task	Syntax

Deleting the settings	`delete maestro`
	Available sub-commands in the '`delete maestro`' command
	`[Global] MyChassis-ch01-01 > delete maestro[ESC][ESC]`
	`delete maestro port VALUE vlan VALUE`
	`delete maestro security-group id VALUE ftw-configuration`
	`delete maestro security-group id VALUE interface VALUE`
	`delete maestro security-group id VALUE management-connectivity`
	`delete maestro security-group id VALUE member VALUE`
	`delete maestro security-group id VALUE serial VALUE`
	`delete maestro security-group new-config`
	`[Global] MyChassis-ch01-01 >`

Notes:

- For more information about the Gaia CLI, see the *R80.20SP Quantum Maestro Gaia Administration Guide*
- After every change, verify (see *"Verifying the Configuration Changes" on page 77*) and then apply (see *"Applying the Configuration Changes" on page 78*) the new configuration.

Applicable configuration procedures are provided below.

Configuring the Number of Maestro Sites

Description

This command configures the number of Maestro sites - Single Site (value 1), or Dual Site (value 2).

Syntax

```
set maestro configuration orchestrator-site-amount {1 | 2}
```

Viewing the Number of Maestro Sites

Description

This command shows the configured number of Maestro sites.

Syntax

```
show maestro configuration orchestrator-site-amount
```

Example

```
MHO> show maestro configuration orchestrator-site-amount
Number of configured Orchestrators in this Maestro deployment is
2.
MHO>
```

Configuring the Site ID in Dual Site Deployment

Description

This command configures the Site ID in Dual Site deployment.

The Quantum Maestro Orchestrators on a site that were installed earlier, must get the ID 1.

The Quantum Maestro Orchestrators on a site that were installed later, must get the ID 2.

Syntax

```
set maestro configuration orchestrator-site-id {1 | 2}
```

Viewing the Site ID in Dual Site Deployment

Description

This command shows the configured Site ID in Dual Site deployment.

Syntax

```
show maestro configuration orchestrator-site-id
```

Creating a New Security Group

Description

This command adds a Security Group with the specified ID on the Quantum Maestro Orchestrator.

Important - You must assign Security Appliances and applicable interfaces. See the corresponding configuration procedures.

Syntax

```
add maestro security-group id <Security Group ID>
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs and the available ID, press the **Tab** key. **Important** - The largest shown ID is the next available ID.

Example - Security Groups with IDS 1 and 2 already exist, ID 3 is the next available ID

```
MHO> add maestro security-group id
1 2 3
MHO> add maestro security-group id 3
Successfully added security group 3
MHO>
```

Deleting a Security Group

Description

This command deletes a Security Group with the specified ID on the Quantum Maestro Orchestrator.

Important - There is no prompt to confirm.

Syntax

```
delete maestro security-group id <Security Group ID>
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.

Example

```
MHO> delete maestro security-group id
1 2 3
MHO> delete maestro security-group id 3
Successfully deleted security group 3
MHO>
```

Adding the Network Configuration to a Security Group

Description

This command adds the Network Configuration in a Security Group with the specified ID.

Syntax

```
set maestro security-group id <Security Group ID> management-
connectivity ipv4-address <Security Group IPv4 Address> mask-
length <1-32> [default-gw <Default Gateway IPv4 Address>]
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
<Security Group IPv4 Address>	Specifies the IPv4 address for the Security Group.
<Default Gateway IPv4 Address>	Specifies the IPv4 address of the Default Gateway for the Security Group.

Example

```
MHO> set maestro security-group id 3 management-connectivity
ipv4-address 192.168.30.40 mask-length 24 default-gw
192.168.30.1
Successfully set management connectivity configuration for
security group 3
MHO>
```

Removing the Network Configuration from a Security Group

Description

This command removes the Network Configuration from a Security Group with the specified ID.

Important - There is no prompt to confirm.

Syntax

```
delete maestro security-group id <Security Group ID> management-
connectivity
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.

Example

```
MHO> delete maestro security-group id[TAB]
1 2 3
MHO> delete maestro security-group id 3 management-connectivity
Successfully deleted management connectivity configuration for
security group 3
MHO>
```

Configuring First Time Wizard settings in a Security Group

Description

This command configures the First Time Wizard settings in a Security Group with the specified ID.

These settings are used to perform initial configuration of Security Appliances assigned to this Security Group.

Warning - If you configure these settings in an existing Security Group (in which you already ran the First Time Configuration Wizard), then the change applies only after you reset each Security Appliance in that Security Group to factory defaults.

Syntax

```
set maestro security-group id <Security Group ID> ftw-
configuration hostname <Hostname> sic <Activation Key> is-vsx
{yes | no}
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`ftw-configuration`	Specifies the First Time Wizard settings for Security Appliances in the Security Group.
`hostname <Hostname>`	Specifies the hostname for Security Appliances.
`sic <Activation Key>`	Specifies the one-time activation key for Security Appliances. The key is between 4 and 127 characters long.
`is-vsx {yes | no}`	Specifies whether to configure the Security Appliances in VSX mode.

Example

```
MHO> set maestro security-group id 3 ftw-configuration hostname
MyGwAppliance sic 123456 is-vsx no
Successfully set FTW configuration to security group 3
MHO>
```

Removing First Time Wizard settings from a Security Group

Description

This command removes the First Time Wizard settings from a Security Group with the specified ID.

Important - There is no prompt to confirm.

Syntax

```
delete maestro security-group id <Security Group ID> ftw-
configuration
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.

Example

```
MHO> delete maestro security-group id[TAB]
1 2 3
MHO> delete maestro security-group id 3 ftw-configuration
Successfully deleted FTW configuration for security group 3
MHO>
```

Assigning One Security Appliance to a Security Group

Best Practice:

1. Before you add Security Appliances to an existing Security Group, enable the SMO Image Cloning feature in the Security Group.
   This feature automatically clones all the required software packages to the new Security Appliances.
   Run in Gaia gClish on the Security Group:

   ```
   set smo image auto-clone state on
   ```

   ```
   show smo image auto-clone state
   ```

2. After you added the Security Appliances, you must disable the SMO Image Cloning feature in the Security Group:

   ```
   set smo image auto-clone state off
   ```

   ```
   show smo image auto-clone state
   ```

Description

This command assigns a Security Appliance with the specified Serial Number to a Security Group with the specified ID.

Important:

- You can assign only Security Appliances of the same model to the same Security Group.
- Security Appliances assigned to the Security Group automatically reboot after you apply the configuration.

Best Practice for Dual Site - Assign the same number (as possible) of Security Appliances from each site to the Security Group. If a failover occurs between the sites, Security Appliances on the new Active site must be able to process all the traffic.

Syntax

```
add maestro security-group id <Security Group ID> serial <Serial Number>
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`serial <Serial Number>`	Assigns one Security Appliance specified by its Serial Number. To see the available Serial Numbers, press the **Tab** key. **Important** - You can assign only appliances of the same model to the same Security Group.

Example

```
MHO> add maestro security-group id 3 serial [TAB]
1234567890
MHO> add maestro security-group id 3 serial 1234567890
Successfully added gw 1234567890 to security group 7
MHO>
```

Removing One Security Appliance from a Security Group

Description

This command removes a Security Appliance with the specified Member ID or Serial Number from a Security Group with the specified ID.

Important:

- The Security Appliance must perform a reset to factory defaults and reboot after you remove it from a Security Group. This is to make sure that no security configuration is left behind.
- There is no prompt to confirm.

Syntax to remove a Security Appliance with the specified Member ID

```
delete maestro security-group id <Security Group ID> member
<Member ID>
```

Syntax to remove a Security Appliance with the specified Serial Number

```
delete maestro security-group id <Security Group ID> serial
<Serial Number>
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`member <Member ID>`	Specifies the Security Appliance by its Member ID in the Security Group. To see the available IDs, press the **Tab** key.
`serial <Serial Number>`	Specifies the Security Appliance by its Serial Number. To see the available Serial Numbers, press the **Tab** key.

Example of removing a Security Appliance with the specified Member ID

```
MHO> delete maestro security-group id 3 member [TAB]
1 2 3 4
MHO> delete maestro security-group id 3 member 4
Successfully deleted member 4 from security group 3
MHO>
```

Example of removing a Security Appliance with the specified Serial Number

```
MHO> delete maestro security-group id 3 serial [TAB]
1234567890
MHO> delete maestro security-group id 3 serial 1234567890
Successfully deleted gw with 1322B01094 from security group 3
MHO>
```

Assigning One Interface to a Security Group

Description

This command assigns an interface with the specified name to a Security Group with the specified ID.

Syntax

```
add maestro security-group id <Security Group ID> interface
<Interface Name>
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`interface <Interface Name>`	Assigns one interface specified by its name. To see the available interfaces, press the **Tab** key.

Example

```
MHO> add maestro security-group id 3 interface [TAB]

eth1-Mgmt2 eth1-Mgmt3 eth1-Mgmt4 eth1-Mgmt6 eth1-Mgmt7 eth1-
Mgmt8
eth1-Mgmt9 eth1-10 eth1-11 eth1-12 eth1-13 eth1-14
eth1-15 eth1-16 eth1-17 eth1-18 eth1-19 eth1-20
eth1-21 eth1-22 eth1-23 eth1-24 eth1-25 eth1-26
eth1-48 eth1-49 eth1-51 eth1-53 eth1-55 eth1-57
eth1-59 eth1-61 eth1-63 eth2-Mgmt1 eth2-Mgmt2 eth2-Mgmt3
eth2-Mgmt4 eth2-06 eth2-07 eth2-08 eth2-09 eth2-10
eth2-11 eth2-12 eth2-13 eth2-14 eth2-15 eth2-16
eth2-17 eth2-18 eth2-19 eth2-20 eth2-21 eth2-22
eth2-23 eth2-24 eth2-25 eth2-26 eth2-48 eth2-49
eth2-51 eth2-53 eth2-55 eth2-57 eth2-59 eth2-61
eth2-63
MHO> add maestro security-group id 3 interface eth1-17
Successfully added interface eth1-17 to security group 3
MHO>
```

Removing One Interface from a Security Group

Description

This command removes an interface with the specified name from a Security Group with the specified ID.

Syntax

```
delete maestro security-group id <Security Group ID> interface
<Interface Name>
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`interface <Interface Name>`	Removes one interface specified by its name. To see the available interfaces, press the **Tab** key.

Example

```
MHO> delete maestro security-group id 3 interface [TAB]

eth1-Mgmt3 eth1-13 eth1-14 eth1-15 eth1-16 eth1-17
MHO> add maestro security-group id 3 interface eth1-17
Successfully deleted interface eth1-17 from security group 3
MHO>
```

Adding VLAN Interfaces on Uplink Ports

Important - Starting from the R80.20SP Jumbo Hotfix Accumulator Take 304 on the Quantum Maestro Orchestrator, it is **not** necessary to configure VLAN interfaces on Uplink ports. For more information, see sk170294.

Description

This command adds a VLAN interface with the specified VLAN Tag on the specified Uplink Port.

Note - There is no prompt to confirm.

Syntax

```
add maestro port <Interface Name> vlan <VLAN Tag ID>
```

Parameters

Parameter	Description
`port <Interface Name>`	Specifies the Uplink port by its name. To see the available ports, press the **Tab** key.
`id <Security Group ID>`	Specifies the VLAN Tag ID between 2 and 4094.

Example

```
MHO> add maestro port 1/20/1 vlan 100
MHO>
```

Viewing VLAN Interfaces on Uplink Ports

Important - Starting from the R80.20SP Jumbo Hotfix Accumulator Take 304 on the Quantum Maestro Orchestrator, it is **not** necessary to configure VLAN interfaces on Uplink ports. For more information, see sk170294.

- R80.20SP Jumbo Hotfix Accumulator Take 304 and above:

  See *"Configuring VLAN Interfaces on Uplink Ports" on page 124*.

  #### Description

  This command shows the Security Group configuration, including VLAN interfaces configured on the Uplink Ports.

  #### Syntax

  ```
  show maestro security-group id <Security Group ID>
  ```

  #### Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the ID of the Security Group. To see the existing IDs, press the **Tab** key.

- R80.20SP Jumbo Hotfix Accumulator Take 302 and lower, or R80.20SP:

  #### Description

  This command shows VLAN interfaces configured on the specified Uplink Port.

  #### Syntax

  ```
  show maestro port <Interface Name> vlans
  ```

Parameters

Parameter	Description
`port <Interface Name>`	Specifies the Uplink port by its name. To see the available ports, press the **Tab** key.

Example

```
MHO> add maestro port 1/20/1 vlan 100
MHO> add maestro port 1/20/1 vlan 200
MHO>
MHO> show maestro port 1/20/1 vlans
Port 1/20/1 vlans are: 100 200
MHO>
```

Removing VLAN Interfaces from Uplink Ports

Important - Starting from the R80.20SP Jumbo Hotfix Accumulator Take 304 on the Quantum Maestro Orchestrator, it is **not** necessary to configure VLAN interfaces on Uplink ports. For more information, see sk170294.

Description

This command removes a VLAN interface with the specified VLAN Tag from the specified Uplink Port.

Note - There is no prompt to confirm.

Syntax

```
delete maestro port <Interface Name> vlan <VLAN Tag ID>
```

Parameters

Parameter	Description
`port <Interface Name>`	Specifies the Uplink port by its name. To see the available ports, press the **Tab** key.
`id <Security Group ID>`	Specifies the VLAN Tag ID. To see the available VLAN Tag IDs, press the **Tab** key.

Example

```
MHO> delete maestro port 1/20/1 vlan 100
MHO>
```

Verifying the Configuration Changes

Description

This command shows and verifies the validity of all the configuration changes you made, but did not apply yet to Security Groups or ports.

Best Practice - Run this command after all changes in the configuration of Security Groups or ports.

Syntax

```
show maestro security-group verify-new-config
```

Example 1 - No changes were made

```
MHO> show maestro security-group verify-new-config
The following changes will take place:
Temporary topology file not exists
MHO>
```

Example 2 - Some changes were made

```
MHO> add maestro security-group id 3
Successfully added security group 3
MHO>
MHO> show maestro security-group verify-new-config
The following changes will take place:
Security Group 1
   - No changes
Security Group 2
   - Removed Gateway 1_2 serial 1234567890. GW is rebooting.
Security Group 3
   - Security group created
   - Added Gateway 1_1 serial 1234567890
   - Added interface eth1-Mgmt4
MHO>
```

Applying the Configuration Changes

Description

This command applies all the configuration changes you made, but did not apply yet to Security Groups or ports.

Important - You must run this command after you make changes in the configuration of Security Groups or ports.

Syntax

```
set maestro security-group apply-new-config
```

Example

```
MHO> set maestro security-group apply-new-config
You are about to perform "set maestro security-group apply-new-
config"
The following changes will take place:
Security Group 1
   - No changes

Are you sure? (Y - yes, any other key - no) y

"set maestro security-group apply-new-config" requires auditing
Enter your full name: johndoe
Enter reason for "set maestro security-group apply-new-config"
[Configuration]: test
CRITICAL: "set maestro security-group apply-new-config", User:
johndoe, Reason: test
Are you sure? (Y - yes, any other key - no) y

Action Summary
--------------

Security Group 1
   - No changes
MHO>
```

Deleting Configuration Changes That Were Not Applied Yet

Description

This command deletes all the configuration changes you made, but did not apply yet to Security Groups or ports.

Important - There is no prompt to confirm.

Syntax

```
delete maestro security-group new-config
```

Example

```
MHO> delete maestro security-group new-config
Successfully deleted new topology configuration
MHO>
```

Configuring the Port Settings

Description

These commands let you configure different settings on the Quantum Maestro Orchestrator's ports.

Syntax

```
set maestro port <Port ID>
      admin-state {up | down}
      mtu 68-10236
      qsfp-mode {1G | 10G | 4x10G | 4x25G | 40G | 100G}
      type {downlink | uplink | management | site_sync} [no-
confirmation]
```

Parameters

Parameter	Description
<Port ID>	Specifies the port to configure. The format is three numbers separated with a slash: *<Quantum Maestro Orchestrator ID>/<Port Label>/<Port Split ID>* Examples: ■ 1/3/1 ■ 2/20/1 Notes: ■ *<Quantum Maestro Orchestrator ID>* is 1 if you connect only one Quantum Maestro Orchestrator. When you connect two Quantum Maestro Orchestrators for redundancy, the *<Quantum Maestro Orchestrator ID>* is 1 on the first Quantum Maestro Orchestrator and 2 on the second Quantum Maestro Orchestrator. ■ *<Port Label>* is the number of the physical port on the front panel. On MHO-140, there are exceptions for ports 51, 53, 55, and 56. ■ The default value of the *<Port Split ID>* is 1, if you did not split the port with a breakout cable. ■ To see the available Port IDs, enter the command `set maestro port` and press the **Tab** key. ■ To see the Port IDs and the names Gaia OS assigned to them, connect to the Gaia Portal on the Quantum Maestro Orchestrator and click **Orchestrator** page. For the default mapping, see the *Quantum Maestro Getting Started Guide* - Section *Maestro Hyperscale Orchestrator Ports and Gaia OS Interfaces*.

Parameter	Description
`admin-state`	Configures the port administrative state: ■ `up` - Enabled ■ `down` - Disabled **Important:** ■ This change does **not** survive reboot of the Orchestrator (a fix for this known limitation MBS-11339 is planned for a future Take of the R80.20SP Jumbo Hotfix Accumulator). ■ By design, in Dual Site, when you run this command on one of the Orchestrators, the corresponding port on the peer Orchestrator on the other site changes its state in the same way. For more information, see sk175549.
`mtu`	Configures the port MTU. Valid range: 68 - 10236 bytes. Default: 10236 bytes.
`qsfp-mode`	Configures the QSFP mode: ■ `1G` - Port works with 1 GbE speed (only 10 GbE ports support this mode) ■ `10G` - Port works with 10 GbE speed ■ `4x10G` - Split of a 40 GbE port into four ports that work with 10 GbE speed each ■ `4x25G` - Support for this mode is planned ■ `40G` - Port works with 40 GbE speed ■ `100G` - Port works with 100 GbE speed **Important** ■ On MHO-170 ports, you can configure only these modes: • Ports with odd <*Port Label*> numbers (1, 3, 5, and so on) - `4x10G`, `40G`, or `100G` • Ports with even <*Port Label*> numbers (2, 4, 6, and so on) - `40G` or `100G` ■ On MHO-140 ports, you can configure only these port modes: • Ports with the <*Port Label*> from 1 to 48 - `1G` or `10G` • Ports with the <*Port Label*> from 49, 51, 53, and 55 - `4x10G`, `40G`, or `100G` • Ports with the <*Port Label*> from 50, 52, 54, and 56 - `40G` or `100G`

Parameter	Description
`type`	Configures the port type: ■ `downlink` - Connects to Check Point Security Appliances ■ `uplink` - Connects to external and internal production networks ■ `management` - Connects to Management Server that manages the applicable Security Group ■ `site_sync` - External synchronization in Dual Site deployment The `no-confirmation` parameter is optional. If specified, the command does not ask you for confirmation and audit information. **Important:** ■ On MHO-170, you can configure only these port types: • Port 1 and Port 2 only as `management` or as `downlink` • Ports 3 and higher only as `uplink`, `downlink`, `site_sync`, or `ssm_sync` (for intra-site sync redundancy) ■ On MHO-140, you can configure only these port types: • Ports 1 - 4 only as `management` or as `downlink` • Ports 5 and higher only as `uplink`, `downlink`, `site_sync`, or `ssm_sync` (for intra-site sync redundancy) ■ You cannot change the type of the dedicated Internal Synchronization port: • MHO-170 - Port 32 • MHO-140 - Port 48 ■

Example 1 - Viewing all available ports

```
MHO> set maestro port [TAB]
1/42/1 1/48/1 1/43/1 1/55/1 1/56/1 1/49/1 1/51/1 1/24/1 1/25/1
1/26/1 1/27/1 1/20/1 1/21/1 1/22/1 1/23/1 1/46/1 1/47/1 1/44/1
1/45/1 1/28/1 1/29/1 1/40/1 1/41/1 1/1/1 1/3/1 1/2/1 1/5/1
1/4/1 1/7/1 1/6/1 1/9/1 1/8/1 1/50/1 1/39/1 1/38/1 1/54/1
1/11/1 1/10/1 1/13/1 1/12/1 1/15/1 1/14/1 1/17/1 1/16/1 1/19/1
1/18/1 1/31/1 1/30/1 1/37/1 1/36/1 1/35/1 1/34/1 1/33/1 1/52/1
1/32/1 1/53/1
MHO>
```

Example 2 - Changing the port administrative state

```
MHO> set maestro port 1/20/1 admin-state down
You are about to perform "set maestro port 1/20/1 admin-state
down"
Action might lead to traffic impact

Are you sure? (Y - yes, any other key - no) y
Successfully set port 20 admin-state to down
MHO>
```

Example 3 - Changing the port MTU

```
MHO> set maestro port 1/20/1 mtu 10236
You are about to perform "set maestro port 1/20/1 mtu 10236"
Action might lead to traffic impact

Are you sure? (Y - yes, any other key - no) y
Successfully set port 20 mtu to 10236
MHO>
```

Example 4 - Changing the port QSFP mode

```
MHO> set maestro port 1/20/1 qsfp-mode 10G
You are about to perform "set maestro port 1/20/1 qsfp-mode 10G"
Action might lead to traffic impact

Are you sure? (Y - yes, any other key - no) y
Successfully set port 20 qsfp-mode to 10G success
MHO>
```

Example 5 - Changing the port type

```
MHO> set maestro port 1/20/1 type uplink
You are about to perform "set maestro port 1/20/1 type uplink"
Are you sure? (Y - yes, any other key - no) y

"set maestro port 1/20/1 type uplink" requires auditing
Enter your full name: johndoe
Enter reason for "set maestro port 1/20/1 type uplink" [Maintenance]: test
WARNING: "set maestro port 1/20/1 type uplink", User: johndoe, Reason: test
Are you sure? (Y - yes, any other key - no) y

Successfully set port 1/20/1 type to uplink
MHO>
MHO> exit
[Expert@MHO:0]#
```

Example 6 - Changing the port type with automatic confirmation

```
MHO> set maestro port 1/20/1 type uplink no-confirmation
You are about to perform "set maestro port 1/20/1 type uplink no-confirmation"
Are you sure? (Y - yes, any other key - no) y

"set maestro port 1/20/1 type uplink no-confirmation" requires auditing
Enter your full name: johndoe
Enter reason for "set maestro port 1/20/1 type uplink no-confirmation" [Maintenance]: test
WARNING: "set maestro port 1/20/1 type uplink no-confirmation", User: johndoe, Reason: test

Successfully set port 1/20/1 type to uplink
MHO>
MHO> exit
[Expert@MHO:0]#
```

Viewing the Port Settings

Description

These commands show the configured settings on the Quantum Maestro Orchestrator's ports.

Syntax

```
show maestro port <Port ID>
      admin-state
      mtu
      optic-info
      qsfp-mode
      type
      vlans
```

Parameters

Parameter	Description
<Port ID>	Specifies the port to configure. The format is three numbers separated with a slash: *<Quantum Maestro Orchestrator ID>/<Port Label>/<Port Split ID>* Examples: ■ 1/3/1 ■ 1/54/1 Notes: ■ If the port is not split with a breakout cable, then the default value of the *<Port Split ID>* is 1. ■ To see the available Port IDs, press the **Tab** key. ■ To see the Port IDs and the names Gaia OS assigned to them, connect to the Gaia Portal on the Quantum Maestro Orchestrator and click **Orchestrator** page. For the default mapping, see the *Quantum Maestro Getting Started Guide* - Section *Maestro Hyperscale Orchestrator Ports and Gaia OS Interfaces*.
admin-state	Shows the port administrative state: ■ up - Enabled ■ down - Disabled
mtu	Shows the port MTU.
optic-info	Shows the information about the QSFP transceiver.
qsfp-mode	Shows the QSFP mode: ■ 1G - Port works with 1 GbE speed (only 10 GbE ports support this mode) ■ 10G - Port works with 10 GbE speed ■ 4x10G - Split of a 40 GbE port into four ports that work with 10 GbE speed each ■ 4x25G - Support for this mode is planned ■ 40G - Port works with 40 GbE speed ■ 100G - Port works with 100 GbE speed

Parameter	Description
`type`	Shows the port type: ■ `downlink` - Connects to Check Point Security Appliances ■ `uplink` - Connects to external and internal production networks ■ `management` - Connects to Management Server that manages the applicable Security Group
`vlans`	Shows the VLAN IDs configured on this port.

Example 1 - Viewing all available ports

```
MHO> show maestro port [TAB]
1/42/1 1/48/1 1/43/1 1/55/1 1/56/1 1/49/1 1/51/1 1/24/1 1/25/1
1/26/1 1/27/1 1/20/1 1/21/1 1/22/1 1/23/1 1/46/1 1/47/1 1/44/1
1/45/1 1/28/1 1/29/1 1/40/1 1/41/1 1/1/1 1/3/1 1/2/1 1/5/1
1/4/1 1/7/1 1/6/1 1/9/1 1/8/1 1/50/1 1/39/1 1/38/1 1/54/1
1/11/1 1/10/1 1/13/1 1/12/1 1/15/1 1/14/1 1/17/1 1/16/1 1/19/1
1/18/1 1/31/1 1/30/1 1/37/1 1/36/1 1/35/1 1/34/1 1/33/1 1/52/1
1/32/1 1/53/1
MHO>
```

Example 2 - Viewing the port administrative state

```
MHO> show maestro port 1/4/1 admin-state
Port 1/4/1 admin-state is down
MHO>

MHO> show maestro port 1/27/1 admin-state
Port 1/27/1 admin-state is up
MHO>
```

Example 3 - Viewing the port MTU

```
MHO> show maestro port 1/27/1 mtu
Port 27 mtu is 10236
MHO>
```

Example 4 - Viewing the QSFP transceiver information

```
MHO> show maestro port 1/27/1 optic-info
 Port:27
Vendor Name:Gigalight
Serial Number:GE18190022
Part Number:GPP-PC192-3001CP
Check Point Part Number:NIY4471
Enforcement:Supported
Check Point SKU:CPAC-DAC-10G-1M-B
Material ID:320904
Product Type:10GBASE-CU-1M
Speed:10G
MHO>
```

Example 5 - Viewing the port QSFP mode

```
MHO> show maestro port 1/27/1 qsfp-mode
Port 27 qsfp-mode is 10G
MHO>
MHO> show maestro port 1/55/1 qsfp-mode
Port 55 qsfp-mode is 100G
MHO>
```

Example 6 - Viewing the port type

```
MHO> show maestro port 1/1/1 type
Port 1/4/1 type is management
MHO>
MHO> show maestro port 1/27/1 type
Port 1/27/1 type is downlink
MHO>
MHO> show maestro port 1/55/1 type
Port 1/55/1 type is uplink
MHO>
```

Example 7 - Viewing the VLAN IDs

```
MHO> show maestro port 1/20/1 vlans
Port 1/20/1 vlans are: 100 200
MHO>
```

Viewing the Security Group Settings

Description

This command shows the Security Group settings on the Quantum Maestro Orchestrator.

Syntax

```
show maestro security-group id <Security Group ID>
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.

Example

```
MHO> show maestro security-group id 1
name: 1
 - uplinks:
  - eth1-05:
   - physical: Port 1/5/1
  - eth1-Mgmt1:
   - physical: Port 1/1/1
  - eth2-05:
   - physical: Port 2/5/1
 - mgmt_ip: 192.168.19.52
 - sic_pass: 12345
 - hostname: MyGW1
 - default_gw: 192.168.19.1
 - is_vsx: false
 - gateways:
  - 1:
   - serial: 2222222222
   - model: Check Point 16000
  - 3:
   - serial: 3333333333
   - model: Check Point 16000
  - 2:
   - serial: 4444444444
   - model: Check Point 16000
  - 4:
   - serial: 5555555555
   - model: Check Point 16000
 - mgmt_netmask: 24
MHO>
```

Configuring Gaia Settings of a Security Group

This section provides instructions for configuring Gaia settings of a Security Group.

Configuring Gaia Settings of a Security Group in Gaia Portal

Step	Instructions
1	With a web browser, connect to the Gaia Portal of the Security Group: `https://<IP Address of Security Group>` **Important** - This connection goes through the Quantum Maestro Orchestrator's management interface you assigned to this Security Group.
2	Log in with these default credentials: ■ Username - `admin` ■ Password - `admin`
3	Change the default Gaia password to a new password: a. From the left tree, click **User Management > Users**. b. Select the **admin** user. c. Click **Reset Password**. d. Enter the new password. e. Click **OK**.
4	From the left tree, click **Network Management > Network Interfaces**.
5	Configure the applicable settings (for example, create a Bond or a VLAN interface) and IP addresses for the Uplink ports. **Important** - In VSX mode, you must configure all IP addresses in SmartConsole only.
6	Configure other applicable Gaia settings. For example: Time Zone, DNS servers, Proxy server, Static Routes.

For more information, see the *R80.20SP Quantum Maestro Gaia Administration Guide*.

Configuring Gaia Settings of a Security Group in Gaia gClish

Note - The commands you run in the Gaia gClish apply to all Security Appliances in this Security Group.

Step	Instructions
1	Connect to the command line of the Security Group over SSH at *<IP Address of Security Group>*. When you log in, the Gaia gClish opens by default. **Important** - This connection goes through the Quantum Maestro Orchestrator's management interface you assigned to this Security Group.

Step	Instructions
2	Log in with these default credentials: ■ Username - `admin` ■ Password - `admin`
3	Change the default Gaia password to a new password: `set user admin password`
4	Configure the applicable settings (for example, create a Bond or a VLAN interface) and IP addresses for the Uplink ports. **Important** - In VSX mode, you must configure all IP addresses in SmartConsole only.
5	Configure other applicable Gaia settings. For example: Time Zone, DNS servers, Proxy server, Static Routes.

For more information, see:

- *R80.20SP Quantum Maestro Gaia Administration Guide*
- *"Connecting to a Specific Security Group Member (member)" on page 131*

Configuration in SmartConsole

Configuring a Security Gateway object and its policy

1. **Create one Security Gateway object**

   You can configure a Security Gateway object in SmartConsole in one of these modes - **Wizard Mode**, or **Classic Mode**:

   Configuring a Security Gateway object in SmartConsole in Wizard Mode

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.

Step	Instructions
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New (✳) > Gateway**. ■ In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > New Gateway**. ■ In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > Gateway**.
4	In the **Check Point Security Gateway Creation** window, click **Wizard Mode**.
5	On the **General Properties** page: a. In the **Gateway name** field, enter a name for this Security Gateway object. b. In the **Gateway platform** field, select **Maestro**. c. In the **Gateway IP address** section, enter the same IPv4 address that you configured for the Security Group on the Quantum Maestro Orchestrator. d. Click **Next**.
6	On the **Trusted Communication** page: a. Select **Initiate trusted communication now**, enter the same Activation Key you entered in the **First Time Wizard settings** of the Security Group on the Quantum Maestro Orchestrator. b. Click **Next**.
7	On the **End** page: a. Examine the **Configuration Summary**. b. Select **Edit Gateway properties for further configuration**. c. Click **Finish**. **Check Point Gateway** properties window opens on the **General Properties** page.
8	On the **Network Security** tab, enable the desired Software Blades. **Important** - Do **not** select anything on the **Management** tab.
9	Click **OK**.
10	Publish the SmartConsole session.

Configuring a Security Gateway object in SmartConsole in Classic Mode

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✶) **> Gateway**. ■ In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > New Gateway**. ■ In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > Gateway**.
4	In the **Check Point Security Gateway Creation** window, click **Classic Mode**. **Check Point Gateway** properties window opens on the **General Properties** page.
5	In the **Name** field, enter a name for this Security Gateway object.
6	In the **IPv4 address** and **IPv6 address** fields, enter the same IPv4 address that you configured for the Security Group on the Quantum Maestro Orchestrator.
7	Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group: a. Near the **Secure Internal Communication** field, click **Communication**. b. In the **Platform** field, select **Open server / Appliance**. c. In the **Activation Key** field, enter the same Activation Key you entered in the **First Time Wizard settings** of the Security Group on the Quantum Maestro Orchestrator. d. Click **Initialize**. e. Click **OK**.
8	In the **Platform** section, select the correct options: a. In the **Hardware** field, select **Maestro**. b. In the **Version** field, select **R80.20SP**. c. In the **OS** field, select **Gaia**.

Step	Instructions
9	On the **Network Security** tab, enable the desired Software Blades. **Important** - Do **not** select anything on the **Management** tab.
10	Click **OK**.
11	Publish the SmartConsole session.

For more information, see the *R80.20 Security Management Administration Guide*.

2. **Configure a Security Policy in SmartConsole**

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click **Security Policies**.
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.
4	Create the applicable Access Control Policy.
6	Create the applicable Threat Prevention Policy.
7	Publish the SmartConsole session.

For more information, see:

- *R80.20 Security Management Administration Guide*
- *R80.20 Threat Prevention Administration Guide*
- Applicable *Administration Guides* on the R80.20SP Home Page and R80.20 Home Page.

3. **Install the Security Policy in SmartConsole**

Step	Instructions
1	Install the Access Control Policy on the Security Gateway object: a. Click **Install Policy**. b. In the **Policy** field, select the applicable policy for this Security Gateway object. c. Select only the Access Control Policy. d. Click **Install**.
2	Install the Threat Prevention Policy on the Security Gateway object: a. Click **Install Policy**. b. In the **Policy** field, select the applicable policy for this Security Gateway object. c. Select only the Threat Prevention Policy. d. Click **Install**.

Configuring a VSX Gateway object and its policies

1. **Configure a VSX Gateway object in SmartConsole**

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server or *Main* Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new VSX Gateway object in one of these ways: ■ From the top toolbar, click the **New (✳) > VSX > Gateway**. ■ In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > VSX > New Gateway**. ■ In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Gateway**. The **VSX Gateway Wizard** opens.
4	On the **VSX Gateway General Properties (Specify the object's basic settings)** page: a. In the **Enter the VSX Gateway Name** field, enter the desired name for this VSX Gateway object. b. In the **Enter the VSX Gateway IPv4** field, enter the same IPv4 address that you configured on the **Management Connection** page of the VSX Gateway's First Time Configuration Wizard. c. In the **Enter the VSX Gateway IPv6** field, enter the same IPv6 address that you configured on the **Management Connection** page of the VSX Gateway's First Time Configuration Wizard. d. In the **Select the VSX Gateway Version** field, select **R80.20SP**. e. Click **Next**.
5	On the **Virtual Systems Creation Templates (Select the Creation Template most suitable for your VSX deployment)** page: a. Select the applicable template. b. Click **Next**.

Step	Instructions
6	On the **VSX Gateway General Properties (Secure Internal Communication)** page: a. In the **Activation Key** field, enter the same Activation Key you entered in the **First Time Wizard settings** of the Security Group on the Quantum Maestro Orchestrator. b. In the **Confirm Activation Key** field, enter the same Activation Key again. c. Click **Initialize**. d. Click **Next**.
7	On the **VSX Gateway Interfaces (Physical Interfaces Usage)** page: a. Examine the list of the interfaces - it must show all the Uplink ports you assigned to this Security Group. b. If you plan to connect more than one Virtual System directly to the same Uplink port, you must select **VLAN Trunk** for that physical Uplink port. c. Click **Next**.
8	On the **Virtual Network Device Configuration (Specify the object's basic settings)** page: a. You can select **Create a Virtual Network Device** and configure the first desired Virtual System at this time (we recommend to do this later). b. Click **Next**.
9	On the **VSX Gateway Management (Specify the management access rules)** page: a. Examine the default access rules. b. Select the applicable default access rules. c. Configure the applicable source objects, if needed. d. Click **Next**. **Important** - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.
10	On the **VSX Gateway Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.

Step	Instructions
11	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`
12	Open the VSX Gateway object.
13	On the **General Properties** page, click the **Network Security** tab.
14	Enable the desired Software Blades for the VSX Gateway object itself (context of VS0). Refer to: ■ sk79700: VSX supported features on R75.40VS and above ■ sk106496: Software Blades updates on VSX R75.40VS and above - FAQ ■ Applicable *Administration Guides* on the R80.20SP Home Page and R80.20 Home Page
15	Click **OK** to push the updated VSX Configuration. Click **View Report** for more information.
16	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`
17	Install policy on the VSX Gateway object: a. Click **Install Policy**. b. In the **Policy** field, select the default policy for this VSX Gateway object. This policy is called: `<Name of VSX Gateway object>_VSX` c. Click **Install**.

Step	Instructions
18	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

2. **Configure Virtual Systems and their Security Policies in SmartConsole**

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server, or each *Target* Domain Management Server that should manage each Virtual System.
2	Configure the desired Virtual Systems on this Security Group.
3	Create the applicable Access Control Policy for these Virtual Systems.
4	Create the applicable Threat Prevention Policy for these Virtual Systems.
5	Publish the SmartConsole session.
6	Install the configured Security Policies on these Virtual Systems.
7	Install the Access Control Policy on these Virtual Systems: a. Click **Install Policy**. b. In the **Policy** field, select the applicable policy for the Virtual System object. c. Select only the Access Control Policy. d. Click **Install**.
8	Install the Threat Prevention Policy on these Virtual Systems: a. Click **Install Policy**. b. In the **Policy** field, select the applicable policy for the Virtual System object. c. Select only the Threat Prevention Policy. d. Click **Install**.
9	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

For more information, see:

- *R80.20 Security Management Administration Guide*
- *R80.20SP Quantum Maestro VSX Administration Guide*
- Applicable *Administration Guides* on the R80.20SP Home Page and R80.20 Home Page

Special Configuration Scenarios

This section contains special configuration scenarios:

- Bond interfaces
- VLAN interfaces

Configuring Bond Interface on the Management Ports

Important - If this Security Group is configured in the VSX mode, follow this workflow:

1. In Gaia gClish, temporarily disable the VSX mode:
   ```
   set vsx off
   ```
2. Configure a Bond Interface on the Management Ports as described below.
3. In Gaia gClish, enable the VSX mode:
   ```
   set vsx on
   ```

Use Case - Creating a New Security Group from Scratch

Note - You can perform Steps 2 - 5 in either Gaia Portal (see *"Configuring Security Groups in Gaia Portal" on page 44*), or Gaia Clish (see *"Configuring Security Groups in Gaia Clish" on page 56*).

Step	Instructions
1	Connect to one of the Quantum Maestro Orchestrators.
2	Create a new Security Group: a. In the **Network settings** section, enter a dummy IP address configuration. b. Do not configure the **First Time Wizard settings**.
3	Assign two available management interfaces `eth`*M*`-Mgmt`*X* and `eth`*N*`-Mgmt`*Y* to the Security Group.
4	Assign the applicable Security Appliances to the Security Group.
5	Assign the applicable Uplink ports to the Security Group.
6	Connect through the console port to the Security Appliance with Member ID 1 in this Security Group.
7	Log in to the Expert mode.

Step	Instructions
8	Go to the Gaia gClish: `gclish`
9	Check which `eth#-Mgmt#` interface has the IP address you assigned to the Security Group. In our example, we assume it is `eth`*`M`*`-Mgmt`*`X`*.
10	Add a new Bonding group with this syntax: `add bonding group <`*`Bond ID`*`> mgmt`
11	Add the free `eth`*`N`*`-Mgmt`*`Y`* interface (without an IP address) to the bonding group with this syntax: `add bonding group <`*`Bond ID`*`> mgmt interface eth`*`N`*`-Mgmt`*`Y`*
12	Assign the real IP address (you wish to use for this Security Group) to the Bonding group with this syntax: `set interface magg<`*`Bond ID`*`> ipv4-address <`*`Real IPv4 Address`*`> mask-length <`*`Mask Length`*`>`
13	Set the Bonding group as the new Gaia Management Interface: `set management interface magg<`*`Bond ID`*`>`
14	Delete the dummy IP address from the `eth`*`M`*`-Mgmt`*`X`* interface: `delete interface eth`*`M`*`-Mgmt`*`X`*` ipv4-address`
15	Add the free `eth`*`M`*`-Mgmt`*`X`* interface (without an IP address) to the bonding group with this syntax: `add bonding group <`*`Bond ID`*`> mgmt interface eth`*`M`*`-Mgmt`*`X`*
16	Connect to one of the Quantum Maestro Orchestrators.
17	Make sure the Security Group settings are correct.
18	In a web browser, connect to the Management IP address of the Security Group and complete the First Time Configuration Wizard manually.

Use Case - Editing an Existing Security Group

Step	Instructions
1	Connect to one of the Quantum Maestro Orchestrators.
2	Assign a second available management interface `eth`*`N`*`-Mgmt`*`Y`* to the Security Group. You can perform this step in Gaia Portal (see *"Configuring Security Groups in Gaia Portal" on page 44*), or Gaia Clish (see *"Configuring Security Groups in Gaia Clish" on page 56*). In our example, we assume that the interface `eth`*`M`*`-Mgmt`*`X`* is already assigned.
3	Connect through the console port to the Security Appliance with Member ID 1 in this Security Group.
4	Log in to the Expert mode.
5	Go to the Gaia gClish: `gclish`
6	Change the IP address on the `eth`*`M`*`-Mgmt`*`X`* interface to some dummy IP address: `set interface eth`*`M`*`-Mgmt`*`X`* `ipv4-address <`*`Dummy IPv4 Address`*`> mask-length <`*`Mask Length`*`>`
7	Add a new Bonding group with this syntax: `add bonding group <`*`Bond ID`*`> mgmt`
8	Add the free `eth`*`N`*`-Mgmt`*`Y`* interface (without an IP address) to the bonding group with this syntax: `add bonding group <`*`Bond ID`*`> mgmt interface eth`*`N`*`-Mgmt`*`Y`*
9	Assign the real IP address to the Bonding group with this syntax: `set interface magg<`*`Bond ID`*`> ipv4-address <`*`Real IPv4 Address`*`> mask-length <`*`Mask Length`*`>`
10	Set the Bonding group as the new Gaia Management Interface: `set management interface magg<`*`Bond ID`*`>`

Step	Instructions
11	Delete the dummy IP address from the `eth`*`M`*`-Mgmt`*`X`* interface: `delete interface eth`*`M`*`-Mgmt`*`X`* `ipv4-address`
12	Add the free `eth`*`M`*`-Mgmt`*`X`* interface (without an IP address) to the bonding group with this syntax: `add bonding group <`*`Bond ID`*`> mgmt interface eth`*`M`*`-Mgmt`*`X`*
13	Connect to one of the Quantum Maestro Orchestrators.
14	Make sure the Security Group settings are correct.
15	In SmartConsole: a. From the left navigation panel, click **Gateways & Servers**. b. Open the Security Gateway object. c. From the left tree, click **Network Management**. d. Click **Get Interfaces** > **Get Interfaces With Topology**. e. Examine the configuration and accept it. f. Click **OK**. g. Install the applicable Access Control Policy.

Configuring Bond Interface on Uplink Ports

1. **Assign the applicable Uplink ports to the applicable Security Group**

   You perform this step on one of the Quantum Maestro Orchestrators.

   You can perform this step in either Gaia Portal, or Gaia Clish of the Quantum Maestro Orchestrator.

   In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal on one of the Quantum Maestro Orchestrators.
2	Assign the applicable Uplink ports to the applicable Security Group. See *"Assigning Interfaces to a Security Group" on page 52*.
3	In the bottom left corner, click **Apply**.

   In Gaia Clish

Step	Instructions
1	Connect to the command line on one of the Quantum Maestro Orchestrators.
2	Log in to the Gaia Clish.
3	Assign the applicable Uplink ports to the applicable Security Group. See *"Assigning One Interface to a Security Group" on page 71*.
4	Verify the new configuration. See *"Verifying the Configuration Changes" on page 77*.
5	Apply the new configuration. See *"Applying the Configuration Changes" on page 78*.

2. **Configure the Bond interface on top of the Uplink ports**

   You can perform this step in either Gaia Portal, or Gaia gClish of the Security Group.

In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal of the Security Group.
2	In the navigation tree, click **Network Management** > **Network Interfaces**.
3	Make sure that the slave interfaces, which you wish to add to the Bond interface, do not have IP addresses.
4	For a new bond interface, select **Add** > **Bond**. To edit an existing Bond interface, select the Bond interface and click **Edit**.
5	On the **IPv4** tab, enter the IPv4 address and subnet mask. **Important**: ■ R80.20SP does not support the option **Obtain IPv4 address automatically** (Known Limitation MBS-3246). ■ This step applies only to the Security Group in the Gateway mode. In the VSX mode, you must assign the IP address in SmartConsole in the VSX Gateway object, or applicable Virtual System object.
6	**Optional**: On the **IPv6** tab, enter the IPv6 address and mask length in the applicable fields. **Important**: ■ First, you must enable the IPv6 Support and reboot (see the "System Configuration" section of the *R80.20SP Quantum Maestro Gaia Administration Guide*. ■ R80.20SP does **not** support IPv6 Address on Gaia Management Interface (Known Limitation 01622840). ■ R80.20SP does **not** support the option **Obtain IPv6 address automatically** (Known Limitation MBS-3246). ■ This step applies only to the Security Group in the Gateway mode. In the VSX mode, you must assign the IP address in SmartConsole in the VSX Gateway object, or applicable Virtual System object.

Step	Instructions
7	On the **Bond** tab: a. Select or enter a **Bond Group ID**. This parameter is an integer between 0 and 1024. b. Select the slave interfaces from the **Available Interfaces** list and then click **Add**. **Note** - Make sure that the slave interfaces do not have any IP addresses or aliases configured. c. Select an **Operation Mode**: ■ **Round Robin** (default) - Bond uses all slave interfaces sequentially (High Availability + Load Sharing) ■ **Active-Backup** - Bond uses one slave interface at a time (High Availability) ■ **XOR** - Bond uses slave interfaces based on a hash function (High Availability + Load Sharing) ■ **802.3ad** - Dynamic bonding according to IEEE 802.3ad (Load Sharing)
8	On the **Advanced** tab: a. Configure the required **MTU** for your network (if not sure, leave the default value). b. Configure the **Monitor Interval** - How much time to wait between checking each slave interface for link-failure. The valid range is 1-5000 ms. The default is 100 ms. c. Configure the **Down Delay** - How much time to wait, after sending a monitor request to a slave interface, before bringing down the slave interface. The valid range is 1-5000 ms. The default is 200 ms. d. Configure the **Up Delay** - How much time to wait, after sending a monitor request to a slave interface, before bringing up the slave interface. The valid range is 1-5000 ms. The default is 200 ms.

Step	Instructions
9	Additional configuration settings are available depending on the selected Bond Operation Mode: ■ If you selected the **Round Robin** bond operation mode, then there are no additional configuration settings. ■ If you selected the **Active-Backup** bond operation mode, then select the **Primary Interface**. ■ If you selected the **XOR** bond operation mode, then select the **Transmit Hash Policy** - the algorithm for slave interface selection according to the specified TCP/IP Layer. Select either **Layer 2** (uses XOR of the physical interface MAC address), or **Layer 3+4** (uses Layer 3 and Layer 4 protocol data). ■ If you selected the **802.3ad** bond operation mode, then perform these two steps: a. Select the **Transmit Hash Policy** - the algorithm for slave interface selection according to the specified TCP/IP Layer. Select either **Layer 2** (uses XOR of the physical interface MAC address), or **Layer 3+4** (uses IP addresses and Ports). b. Select the **LACP Rate** - how frequently the LACP partner should transmit LACPDUs. Select **Slow** (every thirty seconds), or **Fast** (every one second).
10	Click **OK**.

In Gaia gClish

Step	Instructions
1	Make sure that the physical slave interfaces do not have IP addresses.
2	Add a new bonding group: `add bonding group <Bond Group ID>`
3	Set the state of the physical slave interfaces to **UP**: `set interface <Name of Physical Interface> state on`
4	Add slave interfaces to the bonding group: `add bonding group <Bond Group ID> interface <Name of Slave Interface>`

Step	Instructions

5	Configure the bond operating mode:
	`set bonding group <Bond Group ID> mode`
	`round-robin`
	`active-backup [primary <Name of Slave Interface>]`
	`xor xmit-hash-policy {layer2 | layer3+4}`
	`<!-- 8023AD [lacp-rate {slow | fast}] -->`

6	Configure other bond parameters: primary interface, media monitoring, and delay rate.
7	Examine the bonding group configuration: `show bonding {group <Bond Group ID> | groups}`
8	Save the configuration.

For more information, see the *R80.20SP Quantum Maestro Gaia Administration Guide*.

3. **Configure the Security Gateway or VSX Gateway object in SmartConsole**

- If you already created a **Security Gateway** object for this Security Group:

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the applicable Security Gateway object.
4	From the left tree, click **Network Management**.
5	Click **Get Interfaces > Get Interfaces Without Topology**.
6	Click **OK**.
7	Install the Access Control Policy on this Security Gateway object.

- If you already created a **VSX Gateway** object for this Security Group:

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the applicable VSX Gateway object.
4	From the left tree, click **Physical Interfaces**.
5	Click **Add**.
6	Add the new interface. **Important** - Enter the same name (case sensitive) you see in the Gaia settings of this Security Group.
7	Click **OK**.
8	Install the Access Control Policy on this VSX Gateway object.
9	Configure the Bond interface in the applicable Virtual System.
10	Install the Access Control Policy on the applicable Virtual System object.

Note - For more information, see the *R80.20SP Quantum Maestro VSX Administration Guide*.

Configuring VLAN Interfaces on top of a Bond Interface on Uplink Ports

In This Section:

This section shows how to configure VLAN Interfaces on top of a Bond Interface that is configured on Uplink Ports.

Procedure

1. **Add the required VLAN tags and assign the Uplink ports to the applicable Security Group**

   You can perform this step in either Gaia Portal, or Gaia Clish of the Quantum Maestro Orchestrator.

   In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal on one of the Quantum Maestro Orchestrators.
2	Add VLAN tags on the applicable Uplink Ports. See *"Adding VLAN Interfaces on Uplink Ports" on page 54*.
3	Assign the applicable Uplink ports with VLAN tags to the applicable Security Group. See *"Assigning Interfaces to a Security Group" on page 52*.
4	In the bottom left corner, click **Apply**.

   In Gaia Clish

Step	Instructions
1	Connect to the command line on one of the Quantum Maestro Orchestrators.
2	Log in to the Gaia Clish.
3	Add VLAN tags on the applicable Uplink Ports. See *"Adding VLAN Interfaces on Uplink Ports" on page 73*.

Step	Instructions
4	Assign the applicable Uplink ports to the applicable Security Group. See *"Assigning One Interface to a Security Group" on page 71*.
5	Verify the new configuration. See *"Verifying the Configuration Changes" on page 77*.
6	Apply the new configuration. See *"Applying the Configuration Changes" on page 78*.

2. **Configure the Bond interface and VLAN interfaces on the Bond interface in the Security Group**

   You can perform this step in either Gaia Portal, or Gaia gClish of the Security Group.

   In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal of the Security Group.
2	Configure the Bond interface on top of the Uplink ports.
3	Add the same VLAN interfaces on the Bond interface, which you added in the Quantum Maestro Orchestrator.
4	In Gateway mode only: Assign the IP addresses to these VLAN interfaces. **Important** - In VSX mode, you must assign the IP addresses in SmartConsole in the VSX Gateway object or applicable Virtual System object.

   In Gaia gClish

Step	Instructions
1	Connect to the command line of the Security Group.
2	Log in to the Expert mode.
3	Go to the Gaia gClish: `gclish`
4	Configure the Bond interface on top of the Uplink ports.

Step	Instructions
5	Add the same VLAN interfaces on the Bond interface, which you added in the Quantum Maestro Orchestrator.
6	In Gateway mode only: Assign the IP addresses to these VLAN interfaces. **Important** - In VSX mode, you must assign the IP addresses in SmartConsole in the VSX Gateway object or applicable Virtual System object.

For more information, see the *R80.20SP Quantum Maestro Gaia Administration Guide*.

3. **Configure the Security Gateway or VSX Gateway object in SmartConsole**

- If you already created a **Security Gateway** object for this Security Group:

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the applicable Security Gateway object.
4	From the left tree, click **Network Management**.
5	Click **Get Interfaces > Get Interfaces Without Topology**.
6	Click **OK**.
7	Install the Access Control Policy on this Security Gateway object.

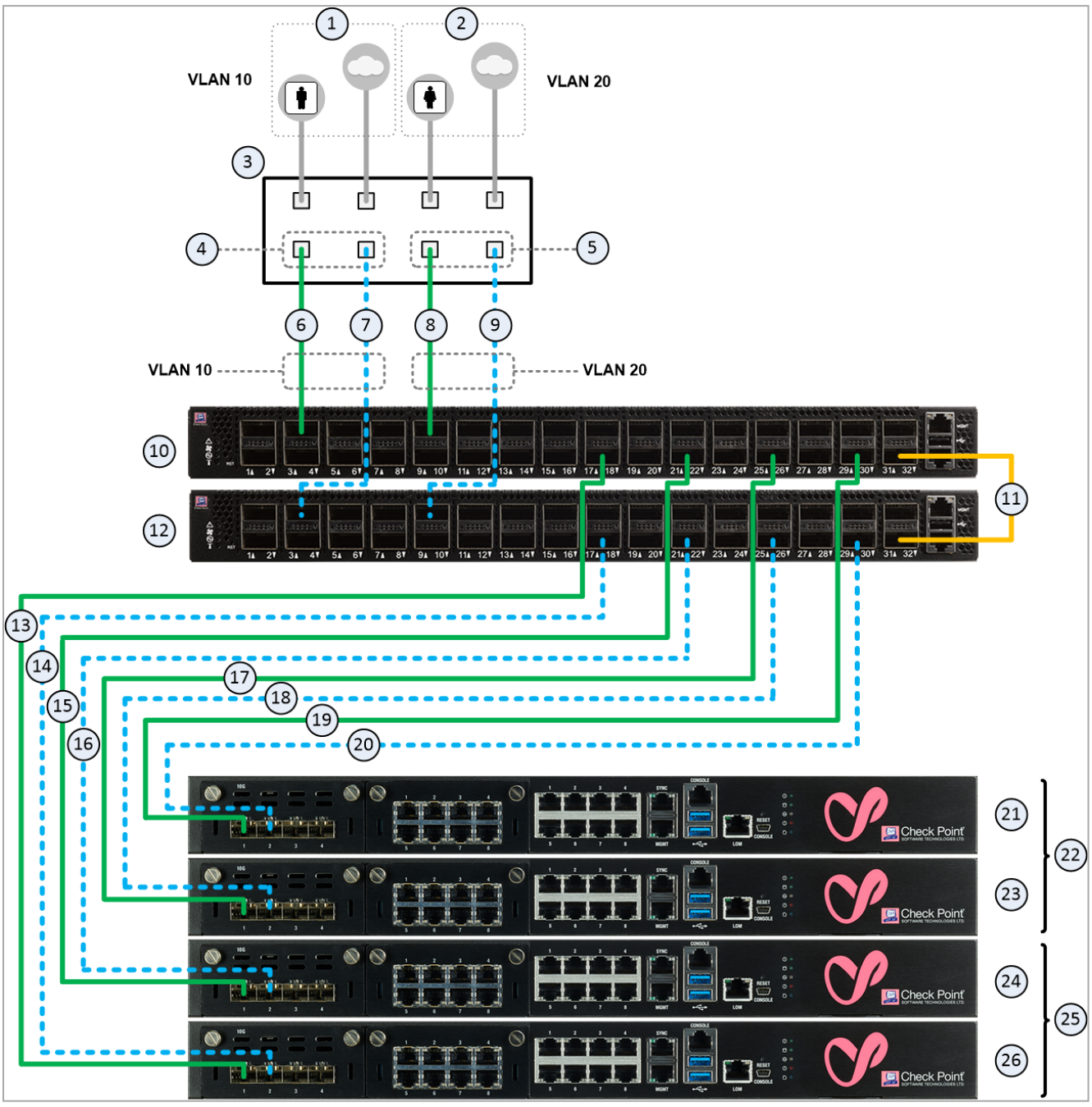
- If you already created a **VSX Gateway** object for this Security Group:

  Note - For more information, see the *R80.20SP Quantum Maestro VSX Administration Guide*.

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the applicable VSX Gateway object.
4	From the left tree, click **Physical Interfaces**.
5	Click **Add**.
6	Add the new Bond interface. **Important** - Enter the same name (case sensitive) you see in the Gaia settings of this Security Group.
7	In the **VLAN Trunk** column, check the box for this Bond interface.
8	Click **OK**.
9	Install the Access Control Policy on this VSX Gateway object.
10	Configure the VLAN interfaces in the applicable Virtual System.
11	Install the Access Control Policy on the applicable Virtual System object.

Example

This example is based on the default configuration of MHO-170:



Explanations

Table: Explanations

Item	Description
1	Network 1 in VLAN 10 connected to ports on the Networking Device (**3**).
2	Network 2 in VLAN 20 connected to ports on the Networking Device (**3**).
3	Networking Device (router or switch) that connects your Network 1 and Network 2 to the Quantum Maestro Orchestrators (**10** and **12**) with Bond interfaces (Link Aggregation).
4	Bond interface that connects Network 1 to the Quantum Maestro Orchestrators (**10** and **12**). This Bond interface provides a redundant Uplink connection for the traffic inspected by the Security Appliances (**26** and **24**) in the applicable Security Group (**25**).
5	Bond interface that connects Network 2 to the Quantum Maestro Orchestrators (**10** and **12**). This Bond interface provides a redundant Uplink connection for the traffic inspected by the Security Appliances (**23** and **21**) in the applicable Security Group (**22**).
6	A DAC cable, Fiber cable (with transceivers), or Breakout cable that connects a first slave of the first Bond (**4**) on the Networking Device (**3**) to the first Quantum Maestro Orchestrator (**10**). This cable connects to the Uplink port 3 (interface `eth1-05`), which must be configured with the VLAN tag 10.
7	A DAC cable, Fiber cable (with transceivers), or Breakout cable that connects a second slave of the first Bond (**4**) on the Networking Device (**3**) to the first Quantum Maestro Orchestrator (**12**). This cable connects to the Uplink port 3 (interface `eth2-05`), which must be configured with the VLAN tag 10.
8	A DAC cable, Fiber cable (with transceivers), or Breakout cable that connects a first slave of the second Bond (**5**) on the Networking Device (**3**) to the second Quantum Maestro Orchestrator (**10**). This cable connects to the Uplink port 9 (interface `eth1-17`), which must be configured with the VLAN tag 20.

Table: Explanations (continued)

Item	Description
9	A DAC cable, Fiber cable (with transceivers), or Breakout cable that connects a second slave of the second Bond (**5**) on the Networking Device (**3**) to the second Quantum Maestro Orchestrator (**12**). This cable connects to the Uplink port 9 (interface `eth2-17`), which must be configured with the VLAN tag 20.
10	First Quantum Maestro Orchestrator.
11	A DAC that connects the dedicated Synchronization ports 32 on the Quantum Maestro Orchestrators (**10** and **12**). **Important** - This connection is only used to synchronize the configuration of Security Groups between the Quantum Maestro Orchestrators.
12	Second Quantum Maestro Orchestrator.
13-20	DAC cables, Fiber cables (with transceivers), or Breakout cables that connect Downlink ports on Quantum Maestro Orchestrators to the Security Appliances.
21-23	All Security Appliances assigned to the Security Group 2.
24-26	All Security Appliances assigned to the Security Group 1.

Example procedure

Step	Instructions
1	Configure the required settings on one of the Quantum Maestro Orchestrators: 1. Connect to one of the Quantum Maestro Orchestrators. 2. Add VLAN tag 10 to the Port 1/3/1 (interface `eth1-05`). 3. Add VLAN tag 10 to the Port 2/3/1 (interface `eth2-05`). 4. Add VLAN tag 20 to the Port 1/9/1 (interface `eth1-17`). 5. Add VLAN tag 20 to the Port 2/9/1 (interface `eth2-17`). 6. Assign the Port 1/3/1 with VLAN tag 10 (interface `eth1-05.10`) to the Security Group 1. 7. Assign the Port 2/3/1 with VLAN tag 10 (interface `eth2-05.10`) to the Security Group 1. 8. Assign the Port 1/9/1 with VLAN tag 20 (interface `eth1-17.20`) to the Security Group 2. 9. Assign the Port 2/9/1 with VLAN tag 20 (interface `eth1-17.20`) to the Security Group 2. 10. Apply the configuration.
2	Configure the required settings in the Security Group 1: 1. Connect to the Gaia of the Security Group 1. 2. Configure a new interface Bond1 on top of the interfaces `eth1-05` and `eth2-05`. 3. Add the VLAN tag 10 on top of the new interface Bond1 (`bond1.10`).
3	Configure the required settings in the Security Group 2: 1. Connect to the Gaia of the Security Group 2. 2. Configure a new interface Bond1 on top of the interfaces `eth1-17` and `eth2-17`. 3. Add the VLAN tag 20 on top of the new interface Bond1 (`bond1.20`).
4	In SmartConsole, add the new interface (`bond1.XX`) to the Security Group object.

Configuring VLAN Interfaces on Uplink Ports

Introduction

In the R80.20SP Jumbo Hotfix Accumulator Take 304, Check Point integrated a major enhancement for the configuration of VLAN interfaces on the Uplink ports of a Quantum Maestro Orchestrator (for more information, see sk170294):

- Increased the number of supported VLAN interfaces on an Orchestrator:
  - No limit for each Uplink port.
  - The total supported number of VLAN interfaces is 9000 (more details are below).
- All distribution modes are now supported on Uplink ports.

  You can use all VLAN interfaces instead of only General + Layer 4 distribution (see sk165172).
- All distribution modes are supported on each VLAN interface on an Uplink port, even if the Uplink port allows only specific VLAN interfaces.
- It is **no** longer required to configure the VLAN interfaces on an Orchestrator.

  Workflow:

  1. Assign the physical interface (e.g., eth1-05) to the applicable Security Group.
  2. Configure the applicable IP address on the physical interface (e.g., eth1-05) or VLAN interfaces (e.g., eth1-05.100) on the Security Group.
  3. In SmartConsole:
     a. Open the Security Gateway object for this Security Group.
     b. From the left tree, click the **Network Management** page.
     c. Click **Get Interfaces** > **Get Interfaces Without Topology** > click **Accept**.
     d. Configure the topology settings for each interface.
     e. Install the Access Control Policy on the Security Gateway object.

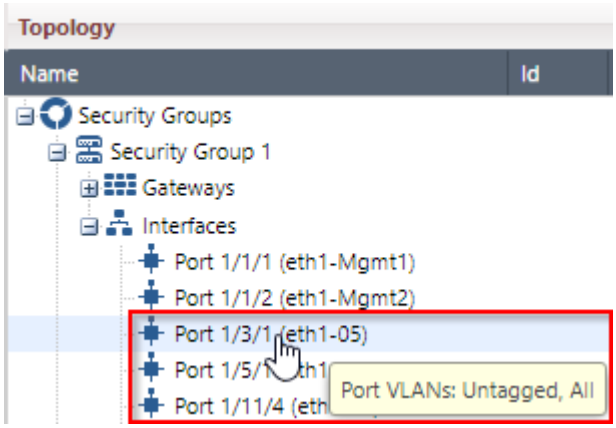
  If there are changes in the configuration of the Security Group interfaces (for example, VLAN interfaces or distribution mode), then the Security Group automatically sends these changes to the Orchestrator. The Security Group does so after a policy installation or a manual change in Gaia gClish.

Viewing VLAN Interfaces on Uplink Ports in Gaia Portal

Step	Instructions
1	On the **Orchestrator** page, in the **Topology** section, expand **Security Groups**.
2	Expand your Security Group.
3	Expand **Interfaces**.
4	Put the mouse cursor on an interface. VLAN information appears in the tooltip.

Note - If this is a Dual Site deployment, and the Security Group contains Security Appliances that are located only at one of the sites (for example, Site 2), then the tooltip that shows VLAN interfaces appears only in Gaia Portal of the Orchestrator (for example, on Site 2) that is located at the same site as Security Appliances.

Example 1



Port:

- Port 1/3/1 (eth1-05)

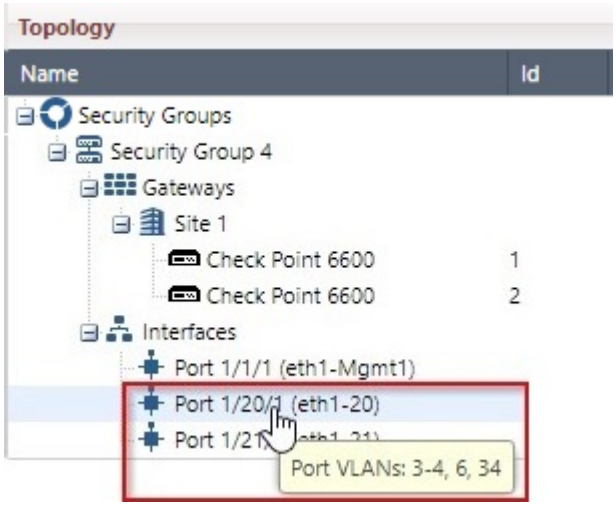
Tooltip:

- Port VLANs: Untagged, All

Explanation:

- The Orchestrator forwards to the Security Group 1 all untagged and all tagged packets that arrive at the Orchestrator port 1/3/1 (eth1-05).
  This is similar to a VLAN Trunk interface configured to allow all VLAN interfaces.

Example 2



Port:

- Port 1/20/1 (eth1-20)

Tooltip:

- Port VLANs: 3-4, 6, 34

Explanation:

- The Orchestrator forwards to the Security Group 4 only packets with VLAN tags 3-4, 6, and 34 that arrive at the Orchestrator port 1/20/1 (eth1-20).
  This is similar to a VLAN Trunk interface configured to allow VLANs 3-4, 6, and 34.

Viewing VLAN Interfaces on Uplink Ports in Gaia Clish

Description

This command shows the Security Group configuration, including VLAN interfaces configured on the Uplink Ports.

Syntax

```
show maestro security-group id <Security Group ID>
```

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the ID of the Security Group. To see the existing IDs, press the **Tab** key.

Configuring More Than 4000 VLAN Interfaces on Orchestrators

If it is necessary to configure more than ~4000 VLAN interfaces on the Orchestrator, we recommend that you configure the physical interface on the Orchestrator as a VLAN trunk interface that allows all untagged and all tagged packet to be forwarded to the Security Group. This makes it possible for an internal automatic optimization to occur.

For a VLAN trunk interface to forward all tagged and all untagged packets, these conditions must be met:

- VLAN Trunk mode must be enabled (see the instructions before how to enable the VLAN Trunk mode).
- The distribution mode of all the VLAN interfaces on a specific physical interface must be the same (because this VLAN optimization occurs for each Orchestrator port).

  Example

  Physical interface on the Orchestrator - eth1-20

  VLAN interfaces - eth1-20.33, eth1-20.44, eth1-20.55, eth1-20.66

  Each of these four VLAN interfaces must have the same distribution mode.

  If one or more of the VLAN interfaces of this specific base interface (eth1-20) have a different distribution than other VLAN interfaces, the internal automatic optimization is disabled. This is part of the design because the total supported number of VLAN interfaces has a limit.

  For example, if the distribution mode of eth1-20.55 is different, then the Orchestrator forwards only the packets with the VLAN tags 33, 44, and 66 are forwarded to the applicable Security Group.

  In the above case, automatic optimization occurs (allows all tagged and untagged packets for eth1-20). Therefore, an interface with this optimization is only considered as one VLAN interface out of total supported 9000 VLAN interfaces for this Orchestrator.

  This means that when this optimization occurs, the full VLAN range can be used on all the Orchestrator interfaces without the limitation of the total supported VLAN interfaces.

To enable the VLAN Trunk mode:

Warnings:

- Do this procedure during a maintenance window.
  No traffic flows through Security Groups while the '`orchd`' process restarts.
- All Orchestrators on your sites must run the same software version.

Step	Instructions
1	Connect to the command line on one of the Orchestrators.
2	Log in to Gaia Clish.
3	Enable the VLAN Trunk mode: `set maestro configuration uplink-trunk-mode state enabled`
4	Examine the status of the VLAN Trunk mode: `show maestro configuration uplink-trunk-mode state`
5	Restart the Maestro daemon: a. Connect to the command line on **each** Orchestrator on your sites. b. Log in to the Expert mode. c. Restart the 'orchd' process: `orchd restart`

License Installation

1. Quantum Maestro Orchestrators do not require a license.
2. Generate a Security Gateway license for the MAC Address of every Security Appliance you connect to a Quantum Maestro Orchestrator.
3. If the applicable license exists in the License Repository on the Check Point Management Server, it installs the licenses automatically.
   - If the Check Point Management Server is connected to the Internet, it pulls the licenses from the User Center.
   - If the Check Point Management Server is not connected to the Internet, then add the licenses manually in the SmartUpdate.
4. If it is necessary to install the license directly on a Security Appliance, these options are available:

   Installing the license on a specific Security Appliance from the Quantum Maestro Orchestrator

Step	Instructions
1	Connect to the command line on the Quantum Maestro Orchestrator. You connect through a dedicated port: ■ In MHO-170 - the **MGMT** port on the front panel (top right corner). ■ In MHO-140 - one of the ports  on the rear panel.
2	Log in to Expert mode.
3	Connect to a specific Security Appliance with this command: `member <Security Group ID> <Member ID>` See *"Connecting to a Specific Security Group Member (member)" on page 131*
4	Run the applicable "`cplic put`" command.

Installing the license in the Gaia OS of the Security Group

Step	Instructions
1	Connect to the Gaia OS of the Security Group.
2	Log in to Expert mode.
3	Connect to a specific Security Appliance with this command: `member <Security Group ID> <Member ID>` See *"Connecting to a Specific Security Group Member (member)" on page 131*
4	Run the applicable `cplic put` command.

Installing the license a specific Security Appliance through the Console port

Step	Instructions
1	Connect to the Security Appliance through the Console port.
2	Log in to the Gaia Clish, or Expert mode.
3	Run the applicable `cplic put` command.

Notes:

- Check Point User Center sends you an email with the full `cplic put` command. You can also see the full syntax in the generated license details in the User Center.
- On the Management Server, each Security Group is one Security Gateway object. Therefore, each Security Group consumes a Management license of one Security Gateway.
- Installation of a Central license with SmartUpdate requires a policy installation on the Security Gateway or VSX Gateway object to propagate the license (see MBS-4510).

Managing Security Groups

This section provides basic information about managing Security Groups.

Connecting to a Specific Security Group Member (member)

You can connect to the command line of a specific Security Group Member in a Security Group in several ways.

Connecting from the Quantum Maestro Orchestrator to a Security Group Member in a Security Group

Step	Instructions
1	Connect to the command line on the Quantum Maestro Orchestrator.

2	Examine the configured Security Group and its Security Group Members.
	■ In the Gaia Clish, run:
	`show maestro security-group id <Security Group ID>`
	■ In the Expert mode, run:
	`clish -c "show maestro security-group id <Security Group ID>"`

3	Make sure to log in to the Expert mode.

4	Connect to a Security Group Member in the Security Group with *one* of these commands:
	`member <Security Group ID> <Member ID>`
	`m <Security Group ID> <Member ID>`

5	Log in.

Example:

```
[Expert@Orch:0]# member 1 3
Moving to member 3 in security group 1 (198.51.101.3)
admin@198.51.101.1's password: *****
Last login: Mon Jan 28 17:05:23 2019 from 198.51.101.126
You have logged into the system.
[Expert@SG1-ch01-03:0]#
```

Connecting from one Security Group Member to another Security Group Member in the same Security Group

Step	Instructions
1	Connect to the command line of the Security Group over SSH at: `<IP Address of Security Group>` **Important** - This connection goes through the Quantum Maestro Orchestrator management interface you assigned to this Security Group.
2	Log in to the Expert mode.

3	Connect to a Security Group Member in the same Security Group with one of these commands:
	`member <Member ID>`
	`m <Member ID>`

Example:

```
[Expert@SG1-ch01-03:0]# m 2
Moving to member 1_2
This system is for authorized use only.
Last login: Mon Jan 28 17:07:45 2019 from 192.0.2.1
You have logged into the system.
[Expert@SG1-ch01-02:0]#
```

Notes:

- To go back to the previous Security Group Member, run the `exit` command.
- You open many SSH sessions to Security Group Members.
- When you connect to a Security Group Member from the Quantum Maestro Orchestrator or from another Security Group Member, the new SSH connection goes over an internal Quantum Maestro Orchestrator network.

Connecting from the Quantum Maestro Orchestrator to a Security Group Member in a Security Group

Step	Instructions
1	Connect to the command line on the Quantum Maestro Orchestrator.

Step	Instructions

2	Examine the configured Security Group and its Security Group Members.
	■ In the Gaia Clish, run:
	`show maestro security-group id <Security Group ID>`
	■ In the Expert mode, run:
	`clish -c "show maestro security-group id <Security Group ID>"`

3	Make sure to log in to the Expert mode.

4	Connect to a Security Group Member in the Security Group with *one* of these commands:
	`member <Security Group ID> <Member ID>`
	`m <Security Group ID> <Member ID>`

5	Log in.

Example:

```
[Expert@Orch:0]# member 1 3
Moving to member 3 in security group 1 (198.51.101.3)
admin@198.51.101.1's password: *****
Last login: Mon Jan 28 17:05:23 2019 from 198.51.101.126
You have logged into the system.
[Expert@SG1-ch01-03:0]#
```

Connecting from one Security Group Member to another Security Group Member in the same Security Group

Step	Instructions
1	Connect to the command line of the Security Group over SSH at: `<IP Address of Security Group>` **Important** - This connection goes through the Quantum Maestro Orchestrator management interface you assigned to this Security Group.
2	Log in to the Expert mode.

Step	Instructions

3	Connect to a Security Group Member in the same Security Group with one of these commands:
	`member <Member ID>`
	`m <Member ID>`

Example:

```
[Expert@SG1-ch01-03:0]# m 2
Moving to member 1_2
This system is for authorized use only.
Last login: Mon Jan 28 17:07:45 2019 from 192.0.2.1
You have logged into the system.
[Expert@SG1-ch01-02:0]#
```

Notes:

- To go back to the previous Security Group Member, run the `exit` command.
- You open many SSH sessions to Security Group Members.
- When you connect to a Security Group Member from the Quantum Maestro Orchestrator or from another Security Group Member, the new SSH connection goes over an internal Quantum Maestro Orchestrator network.

Global Commands

In This Section:

Working with Global Commands *135*

General Global Commands *136*

Global Operating System Commands *144*

Check Point Global Commands *151*

The Gaia operating system includes a set of global commands that apply to all or specified Security Group Members.

Working with Global Commands

Background

- Gaia gClish commands apply globally to all Security Group Members, by default.
- Gaia gClish commands do not apply to Security Group Members that are in the DOWN state in the Security Group.

  If you run a "`set`" command while a Security Group Member is in the DOWN state, the command does not update that Security Group Member.

  The Security Group Member synchronizes its database during startup and applies the changes after reboot.
- Gaia Clish commands apply only to the specific Security Group Member.

  For these commands, see the *R80.20SP Quantum Maestro Gaia Administration Guide*.

Global Commands

Command	Instructions
`auditlog`	■ Enabled by default. ■ All commands are recorded in the audit log. ■ To learn more about the audit log, see *Looking at the Audit Log*.
`config-lock`	■ Protects the Gaia gClish database by locking it. Each Security Group Member has one lock. ■ To set Gaia gClish operations for an Security Group Member, the Security Group Member must hold the "`config-lock`". ■ To set the "`config-lock`", run: `set config-lock on override` ■ Gaia gClish traffic runs on the Sync interface, TCP port 1129.
`blade-range`	■ Runs commands on specified Security Group Members. ■ Runs Gaia gClish embedded commands only on this subset of Security Group Members. ■ We do not recommend that you use the `blade-range` command, because all Security Group Members must have identical configurations.

General Global Commands

Global commands apply to more than one Security Group Member.

These commands are available in Gaia Clish and Gaia gClish:

In Gaia Clish and Gaia gClish	In the Expert mode
`update_conf_file`	`g_update_conf_file`
`global`	`global_help`
`asg_cp2blades`	`asg_cp2blades`
`asg_clear_table`	`asg_clear_table`

Below are some global commands

Viewing the List of Global Commands (global help)

Description

Use the "`global help`" command in Gaia gClish to show the list of global commands you can use in Gaia gClish.

Syntax

```
global help
```

Examples

Example output in Gateway mode

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> global help
Usage: <command_name> [-b SGMs] [-a -l -r --] <native command arguments>
Executes the specified command on specified blades.

Optional Arguments:
  -b   blades: in one of the following formats
               1_1,1_4 or 1_1-1_4 or 1_01,1_03-1_08,1_10
               all (default)
               chassis1
               chassis2
               chassis_active
  -a         : Force execution on all SGMs (incl. down SGMs).
  -l         : Execute only on local blade.
  -r         : Execute only on remote SGMs.

Command list:
snapshot_show_current snapshot_recover fwaccel6_m fwaccel6 fw6 unlock update_conf_file mv fwaccel_m ethtool md5sum dmesg cp
tcpdump cat tail clusterXL_admin reboot ls fwaccel vpn fw netstat cpstop cpstart cplic asg
[Global] MyChassis-ch01-01>
```

Example output in VSX mode

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> global help
Usage: <command_name> [-b SGMs] [-a -l -r --] <native command arguments>
Executes the specified command on specified blades.

Optional Arguments:
  -b   blades: in one of the following formats
               1_1,1_4 or 1_1-1_4 or 1_01,1_03-1_08,1_10
               all (default)
               chassis1
               chassis2
               chassis_active
  -a         : Force execution on all SGMs (incl. down SGMs).
  -l         : Execute only on local blade.
  -r         : Execute only on remote SGMs.

Command list:
cplic cpstart cpstop netstat fw vpn fwaccel ls reboot clusterXL_admin tail cat tcpdump cp dmesg md5sum ethtool fwaccel_m mv
update_conf_file unlock fwaccel6_m snapshot_recover snapshot_show_current asg
[Global] MyChassis-ch01-01>
```

Updating Configuration Files (update_conf_file)

Description

Use these commands to add, update, and remove parameters in configuration files.

Important - After you change the configuration files, you must reboot the Security Group with the "`reboot -b all`" command.

Syntax

Shell	Syntax
Gaia gClish	`update_conf_file <File Name> <Parameter Name>=<Parameter Value>`
Expert mode	`g_update_conf_file <File Name> <Parameter Name>=<Parameter Value>`

Important:

- There must not be a space in front of the equal sign (=).
- There must not be a space after the equal sign (=).

Parameters

Parameter	Description
<File Name>	Full path and name of the configuration file to update You do not need to specify the full path for these files (only specify the file name): ■ `$FWDIR/boot/modules/fwkern.conf` ■ `$PPKDIR/conf/simkern.conf`
<Parameter Name>	Name of the parameter to configure.
<Parameter Value>	New value for the parameter to configure.

Notes:

- These commands work with configuration files in a specified format.
  It is composed of lines, where each line defines one parameter:
  <Parameter Name>=<Parameter Value>
  The `$FWDIR/boot/modules/fwkern.conf` and `$PPKDIR/conf/simkern.conf` files use this format.
- If the specified configuration file does not exist, these commands create it.
- These commansd make the required changes on all Security Group Members.

Examples

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> update_conf_file /home/admin/MyConfFile.txt var1=hello
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var1=hello

[Global] MyChassis-ch01-01> update_conf_file /home/admin/MyConfFile.txt var2=24h
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var2=24h
var1=hello

[Global] MyChassis-ch01-01> update_conf_file /home/admin/MyConfFile.txt var1=goodbye
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var2=24h
var1=goodbye

[Global] MyChassis-ch01-01> update_conf_file /home/admin/MyConfFile.txt var2=
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var1=goodbye
[Global] MyChassis-ch01-01>
```

Setting Firewall Kernel Parameters (g_fw ctl set)

Description

Use these commands in the Expert mode to show or set the values of the specified Firewall kernel parameters.

Syntax for viewing the current value of a kernel parameter

```
g_fw ctl get <Parameter Type> <Parameter Name>
```

Syntax for setting a value of a kernel parameter

```
g_fw ctl set <Parameter Type> <Parameter Name> <Parameter Value>
```

Parameters

Parameter	Description
`get`	Shows the specified parameter and its value.
`set`	Change the parameter value to the specified value.
`<Parameter Type>`	Type of the parameter: ▪ `int` - Accepts integer values ▪ `str` - Accepts string values **Note** - You must enter the correct parameter type.
`<Parameter Name>`	Parameter name to configure.
`<Parameter Value>`	Parameter value to configure.

Note - To make changes persistent, you must manually add the applicable kernel parameters and their values in the `$FWDIR/boot/modules/fwkern.conf` file.
Use the "`g_update_conf_file`" command in the Expert mode.
See *"Updating Configuration Files (update_conf_file)" on page 137*.

For more information, see the *R80.20SP Quantum Maestro Security Gateway Guide* > Chapter *Working with Kernel Parameters on Security Groups*.

Copying Files Between Security Group Members (asg_cp2blades)

Description

Use the "`asg_cp2blades`" command in Gaia gClish or the Expert mode to copy files from the current Security Group Member to another Security Group Member.

Syntax (for Gaia gClish and the Expert mode)

```
asg_cp2blades [-b <SGM IDs>] [-s] <Source Path> [<Destination Path>]
```

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`-r`	Copy folders and directories that contain files.
`-s`	Save a local copy of the old file on each Security Group Member. The copy is saved in the same directory as the new file. The old file has the same name with this at the end: `*.bak.<date>.<time>`
`<Source Path>`	Full path and name of the file to copy.
`<Destination Path>`	Full path of the destination. If not specified, the command copies the file to the relative source file location.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg_cp2blades /home/admin/note.txt
Operation completed successfully
[Global] MyChassis-ch01-01 >
[Global] MyChassis-ch01-01 > cat /home/admin/note.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
hello world
[Global] MyChassis-ch01-01>
```

Deleting Connections from the Connections Table (asg_clear_table)

Description

Use the "`asg_clear_table`" command in Gaia gClish or the Expert mode to delete connections from the Connections table on the Security Group Members.

The command runs up to 15 times, or until there are less than 50 connections left.

Important - If you are connected to the Security Group over SSH, your connection is disconnected.

Syntax (for Gaia gClish and the Expert mode)

```
asg_clear_table [-b <SGM IDs>]
```

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`) **Note** - With this option, you can only select Security Group Members from one Site.

Viewing Information about Interfaces on Security Group Members (show interface)

Description

Use the "`show interface`" command in Gaia gClish to view information about the interfaces on the Security Group Members.

For more information, see the *R80.20SP Quantum Maestro Gaia Administration Guide* > Chapter *Network Management* > Section *Network Interfaces*.

Syntax

```
show interfaces all
show interface <Options>
```

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> show interface eth1-01 ipv4-address
1_01:
ipv4-address 4.4.4.10/24

1_02:
ipv4-address 4.4.4.10/24

1_03:
ipv4-address 4.4.4.10/24

1_04:
ipv4-address 4.4.4.10/24

1_05:
Blade 1_05 is down. See "/var/log/messages".

2_01:
ipv4-address 4.4.4.10/24

2_02:
ipv4-address 4.4.4.10/24

2_03:
ipv4-address 4.4.4.10/24

2_04:
ipv4-address 4.4.4.10/24

2_05:
ipv4-address 4.4.4.10/24
[Global] MyChassis-ch01-01>
```

Global Operating System Commands

Global operating system commands are standard Linux commands that run on all or specified Security Group Members.

When you run a global command in Gaia gClish, the operating system runs a global script that is the standard Linux command on the Security Group Members.

When you run a command in the Expert mode, it works as a standard Linux command.

To use the global command in the Expert mode, run the global command script version as shown in this table:

Gaia gClish Command	Global Command in the Expert mode
`arp`	`g_arp`
`cat`	`g_cat`
`cp`	`g_cp`
`dmesg`	`g_dmesg`
`ethtool`	`g_ethtool`
`ifconfig`	`asg_ifconfig`
`ls`	`g_ls`
`md5sum`	`g_md5sum`
`mv`	`g_mv`
`netstat`	`g_netstat`
`reboot`	`g_reboot`
`tail`	`g_tail`
`tcpdump`	`g_tcpdump`
`top`	`g_top`

Notes:

- The parameters and options for the standard Linux command are available for the global command.
- You can use one or more flags.
- Do **not** use these two flags together in the same command:
  - The "`-l`" flag - to execute the command only on the local Security Group Member
  - The "`-r`" flag - to execute the command only on the remote Security Group Member

Syntax

- In Gaia Clish:

```
<Gaia gClish Command> [-b <SGM IDs>] <Command Options>]
```

- In the Expert mode:

```
<Global Expert mode Command> [-b <SGM IDs>] <Command Options>]
```

Parameters

Parameter	Description
<Gaia gClish Command>	Standard command in Gaia gClish as appears in the table above.
<Global Expert mode Command>	Global command in the Expert mode as appears in the table above.

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`) **Note** - You can only select Security Group Members from one Site with this option.
`<Command Options>`	Standard command options for the specified command.

Below are explanations about some of the global commands.

Global 'ls'

Description

The global `ls` command shows the file in the specified directory on all Security Group Members.

Syntax

- In Gaia Clish:

```
ls [-b <SGM IDs>] <Command Options>]
```

- In the Expert mode:

```
g_ls [-b <SGM IDs>] <Command Options>]
```

Example

This example runs the '`g_ls`' command in the Expert mode on Security Group Members 1_1, 1_2, and 1_3.

The example output shows the combined results for these Security Group Members.

```
[Expert@MyChassis-ch0x-0x:0]# g_ls -b 1_1-1_3,2_1 /var/
-*- 4 blades: 1_01 1_02 1_03 -*-
CPbackup    ace    crash  lib   log   opt       run    suroot
CPsnapshot  cache  empty  lock  mail  preserve  spool  tmp
[Expert@MyChassis-ch0x-0x:0]#
```

Global 'reboot'

Description

The global `reboot` command reboots all Security Group Members.

Syntax

- In Gaia Clish:

  ```
  reboot [-a]
  ```

- In the Expert mode:

  ```
  g_reboot [-a]
  ```

Parameters

Parameter	Description
No Parameters	Reboots all Security Group Members that are in the UP state.
`-a`	Reboots all Security Group Members that in the DOWN and the UP states.

Global 'top'

Description

The global `top` command:

- Shows CPU utilization in real time on Security Group Members.
- Uses the local Security Group Member configuration file (`~/.toprc`) to format the output on the remote Security Group Members.

  The command copies this file to the remote Security Group Members.

Syntax

- In Gaia Clish:

```
top -h
```

```
top [local] [-f [-o <Output File>] [-n <Number of Iterations>]] -b <SGM IDs> [<Command Options>]
```

```
top [local] [s <Output File>] -b <SGM IDs> [<Command Options>]
```

- In the Expert mode:

```
g_top -h
```

```
g_top [local] [-f [-o <Output File>] [-n <Number of Iterations>]] -b <SGM IDs> [<Command Options>]
```

```
g_top [local] [s <Output File>] -b <SGM IDs> [<Command Options>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`local`	Uses the '`top`' configuration file (`~/.toprc`) on the local Security Group Member.
`-f`	Exports the output to a file. Default: `/vat/log/gtop.<Time>`
`-o <Output File>`	Specifies the path and name of the output file. Must use with the "`-f`" parameter.
`-n <Number of Iterations>`	The command saves the output the specified number of times. Default: 1 Must use with the "`-f`" parameter.
`-s <Output File>`	Shows the content of the output file `<Output File>`, in which the command saved its output earlier.
`<Command Options>`	Parameters of the standard `top` command. For more information, see the `top` command documentation.

Configuring the 'g_top' output

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Run: `top`
4	Set the desired view (press **h** to see the built-in help).
5	Press **Shift+W** to save the '`top`' configuration.
6	Run: `g_top`

Global 'arp'

Description

The global `arp` command shows the ARP cache table on all Security Group Members.

Syntax

- In Gaia Clish:

  ```
  arp [-b <SGM IDs>] <Command Options>]
  ```

- In the Expert mode:

  ```
  g_arp [-b <SGM IDs>] <Command Options>]
  ```

Example - ARP table on all interfaces of all Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > arp
1_01:
Address     HWtype  HWaddress           Flags Mask   Iface
192.0.2.2   ether   00:1C:7F:02:04:FE   C            Sync
172.23.9.28 ether   00:14:22:09:D2:22   C            eth1-Mgmt4
192.0.2.3   ether   00:1C:7F:03:04:FE   C            Sync
1_02:
Address     HWtype  HWaddress           Flags Mask   Iface
192.0.2.3   ether   00:1C:7F:03:04:FE   C            Sync
172.23.9.28 ether   00:14:22:09:D2:22   C            eth1-Mgmt4
192.0.2.1   ether   00:1C:7F:01:04:FE   C            Sync
1_03:
Address     HWtype  HWaddress           Flags Mask   Iface
192.0.2.1   ether   00:1C:7F:01:04:FE   C            Sync
172.23.9.28 ether   00:14:22:09:D2:22   C            eth1-Mgmt4
192.0.2.2   ether   00:1C:7F:02:04:FE   C            Sync
[Global] MyChassis-ch01-01 >
```

Check Point Global Commands

These global commands apply to more than one Security Group Member. These global commands let you work with Security Gateway and SecureXL.

fw, fw6

Description

The `fw` and `fw6` commands are global scripts that run the `fw` and `fw6` commands on each Security Group Member.

Syntax

Shell	Syntax
Gaia Clish Gaia gClish	`fw` `fw6`
Expert mode	`g_fw` `g_fw6`

Examples

Example 1

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> fw ctl
-*- 2 blades: 1_01 1_02 -*-
 Usage: fw ctl command args...
 Commands: install, uninstall, pstat, iflist, arp, debug, kdebug, bench
    chain, conn, multik, conntab, fwghtab_bl_stats
[Global] MyChassis-ch01-01 >
```

Example 2

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> fw ctl iflist
-*- 6 blades: 1_01 1_02 1_03 2_01 2_02 2_03 -*-
0 : BPEth0
1 : BPEth1
2 : eth1-Mgmt4
3 : eth2-Mgmt4
4 : eth1-01
5 : eth1-CIN
6 : eth2-CIN
8 : eth2-01
16 : Sync
17 : eth1-Mgmt1
18 : eth2-Mgmt1
[Global] MyChassis-ch01-01 >
```

fw dbgfile

Description

Use the "`fw dbgfile`" commands in Gaia gClish to debug how the Security Group inspect traffic.

Syntax to collect the debug

```
fw dbgfile collect -f <Debug Output File> [-buf <Buffer Size>]
[-m <Debug Module 1> <Debug Flags 1> [-m <Debug Module 2> <Debug
Flags 2>] ... [-m <Debug Module N> <Debug Flags N>]]
```

Syntax to show the collected debug

```
fw dbgfile view [<Debug Output File>] [-o <Debug Output File>]
```

Parameters

Parameter	Description
`collect`	Collects the Security Gateway debug information.
`view`	Shows the collected debug information.
<Debug Output File>	Specifies the full path and the name of the debug output file.
`-buf` *<Buffer Size>*	Specifies the debug buffer size. Always set the maximal size 8200.
`-m` *<Debug Module 1> Debug Flags 1>* `[-m` *<Debug Module 2> <Debug Flags 2>*`]` `...` `[-m` *<Debug Module N> <Debug Flags N>*`]`	Specifies Security Gateway debug modules and debug flags in those modules. You can specify more than one debug module.
`-o` *<Debug Output File>*	Specifies the full path and the name of the debug output file to read.

Examples

Example - Collect debug information

```
[Global] MyChassis-ch01-01 > fw dbgfile collect -f /var/log/debug.txt -buf 8200 -m fw + conn -m kiss + pmdump
```

Example - Show the collected debug information

```
[Global] MyChassis-ch01-01 > fw dbgfile view /var/log/debug.txt
```

Important - For complete debug procedure, see the *R80.20SP Quantum Maestro Security Gateway Guide* > Chapter *Kernel Debug on Security Groups*.

fwaccel, fwaccel6

Description

The `fwaccel` commands control the acceleration for IPv4 traffic.

The `fwaccel6` commands control the acceleration for IPv6 traffic.

Syntax

Shell	Syntax for IPv4	Syntax for IPv6
Gaia Clish Gaia gClish	`fwaccel help`	`fwaccel6 help`
Expert mode	`g_fwaccel help`	`g_fwaccel6 help`

Parameters and Options

For more information, see the *R80.20SP Quantum Maestro Performance Tuning Administration Guide* > Chapter *SecureXL* > Section *SecureXL Commands and Debug* - Subsection *'fwaccel' and 'fwaccel6'*.

Backing Up and Restoring Gaia Configuration

For more information, see the :

- Chapter *Maintenance* > Section *System Backup*.
- Chapter *Maintenance* > Section *Snapshot Management*.

Working with Security Group Gaia gClish Configuration (asg_config)

Description

Use the "`asg_config`" command in Gaia gClish or Expert mode to:

- Show the current Gaia gClish configuration on all SGMs.
- Save the current Gaia gClish configuration of all SGMs to a file.

Use cases:

- Copy the Gaia gClish configuration to a different Chassis.

  For example, you can use the saved configuration from an existing Chassis to configure up a new Chassis.

- Quickly re-configure a Chassis that was reverted to factory defaults.

  Before you revert to the factory default image, save the existing Gaia gClish configuration. Then use it to override the factory default settings.

Syntax

```
asg_config show
asg_config save [-t] [<Output File>]
```

Parameters

Parameter	Description
`show`	Show the existing Gaia gClish configuration.
`save`	Save the current Gaia gClish configuration to a file. If you do not include a path, the output file is saved to this directory: `/home/admin/`
`-t`	Adds a timestamp in Unix Epoch format to the file name.
<Output File>	Specifies the path and name of the output file. If you do not include a path, the output file is saved to this directory: `/home/admin/`

Example - Save the current Gaia gClish configuration to the `/home/admin/myconfig` file

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg_config save -t mycongfig
[Global] MyChassis-ch01-01 > exit
[Expert@MyChassis-ch0x-0x:0]# ls -l ~/mycongfig*
-rw-rw---- 1 admin root 75891 Feb 28 04:38 mycongfig.1551346686
[Expert@MyChassis-ch0x-0x:0]# date -d @1551346686
Thu Feb 28 04:38:06 EST 2019
[Expert@MyChassis-ch0x-0x:0]#
```

Configuring Security Group Members (asg_blade_config)

Description

Use the "`asg_blade_config`" command in the Expert mode to manage Security Group Members:

- Copy the Security Group Member configuration from the local Security Group Member to other Security Group Members in the Security Group
- Change the synchronization start IP address
- Reset the system uptime value
- Get a policy from the Management Server

Syntax

```
asg_blade_config
      fetch_smc
      full_sync <IP Address>
      get_smo_ip
      is_in_pull_conf_group
      is_in_security_group
      pull_config
      reset_sic -reboot_all <Activation Key>
      set_sync_start_ip <Start IP Address>
      upgrade_cu
      upgrade_start <New Version> [cu]
      upgrade_stat
      upgrade_stop
```

Parameters

Parameter	Description
`fetch_smc`	Fetches policy from Management Server and distributes it to all Security Group Members.
`full_sync <IP Address>`	Runs Full Sync with the remote Security Group Member, whose IP address is `<IP Address>`.
`get_smo_ip`	Gets the SMO IP address from the Cluster Control Protocol (CCP) packets sent in the Security Group.
`is_in_pull_conf_group`	Checks whether the Security Group Member is in the Pulling Configuration Group.
`is_in_security_group`	Checks whether the Security Group Member is in the Security Group.
`pull_config`	Pulls configuration from other Security Group Members.
`reset_sic -reboot_all <Activation Key>`	Starts a Secure Internal Communication (SIC) cleanup. You must enter the `<Activation Key>`. You use this key later in SmartConsole to establish Secure Internal Communication.
`set_sync_start_ip <Start IP Address>`	Changes the Sync start IP address of local Security Group Member to `<Start IP Address>`.
`upgrade_cu`	Enables the Connectivity Upgrade mode (runs an iteration).
`upgrade_start <New Version> [cu]`	Starts an upgrade procedure from the current version to the `<New Version>`. The "`cu`" parameter uses the Connectivity Upgrade mode.
`upgrade_stat`	Shows the upgrade procedure information.
`upgrade_stop`	Stops the upgrade procedure.

Troubleshooting the `asg_blade_config` command

To troubleshoot problems associated with the "`asg_blade_config`" command, examine the logs listed in the `$FWDIR/log/blade_config` file.

For example, if a Security Group Member unexpectedly reboots, you can search the log file for the word reboot to learn why.

Working with the Distribution Mode

In This Section:

Background ... 159
Automatic Distribution Configuration (Auto-Topology) ... 160
Manual Distribution Configuration (Manual-General) ... 160
Setting and Showing the Distribution Configuration (set distribution configuration) ... 161
Configuring the Interface Distribution Mode (set distribution interface) ... 163
Showing Distribution Status (show distribution status) ... 165
Running a Verification Test (show distribution verification) ... 167
Configuring the Layer 4 Distribution Mode and Masks (set distribution l4-mode) ... 168

Background

The Quantum Maestro Orchestrator uses the Distribution Mode to assign incoming traffic to Security Group Members in each Security Group.

By default, the Quantum Maestro Orchestrator automatically configures the Distribution Mode.

Supported Distribution Modes

Mode	Instructions
User (Internal)	Packets are assigned to a Security Group Member based on the packet's Destination IP address. If Layer 4 distribution is enabled, SSM assigns packets to a Security Group Member based on the packet's Source Port and the Destination IP address.
Network (External)	Packets are assigned to a Security Group Member based on the packet's Source IP address. If Layer 4 distribution is enabled, SSM assigns packets to a Security Group Member based on the packet's Source IP address and Destination Port.
General	SSMs assign packets to a Security Group Member based on the packet's Source IP address and the Destination IP address. If Layer 4 distribution is enabled, SSMs assign packets to a Security Group Member based on the packet's Source IP address, Source Port, Destination IP address, and Destination Port.

Mode	Instructions
Auto-Topology (Per-Port)	Each port for a Security Group Member is configured separately in the User Mode or Network Mode.

Notes:

- The default mode is **General** and the Layer 4 distribution is enabled.
- The **User** (**(Internal)**) Mode and **Network** (**(External)**) Mode can work together.
  The supported combinations are:
  - User Mode and User Mode
  - User Mode and Network Mode
  - Network Mode and Network Mode

  In many scenarios, it is possible to optimize the combination of the User Mode and Network Mode to pass traffic through same Security Group Member from the two sides.

Automatic Distribution Configuration (Auto-Topology)

By default, Security Groups work in the **General** Mode.

The best Distribution Mode is selected based on the Security Group topology as defined in SmartConsole in the Security Gateway object.

The Distribution Mode is automatically based on these interface types:

- Physical interfaces, except for management and synchronization interfaces
- VLAN
- Bond
- VLAN on top of Bond

Manual Distribution Configuration (Manual-General)

In some deployments, you must manually configure a Distribution Mode to the **General**.

In other cases, it may be necessary to force the system to work in the **General** Mode.

When the Distribution Mode is manually configured (**Manual-General** Mode), the Distribution Mode of each SSM is **General**.

In this configuration, the topology of the interfaces is irrelevant.

Best Practice - Do **not** manually change the Distribution Mode of a Virtual System. This can cause performance degradation.

Setting and Showing the Distribution Configuration (set distribution configuration)

Use these Gaia gClish commands on a Security Group to set and show the distribution configuration.

Important - If the Security Group runs in a VSX mode, run the commands in the context of VS0 only. The commands apply immediately across all Virtual Systems.

Syntax to show the Distribution Configuration

```
show distribution configuration
```

Syntax to set the Distribution Configuration

```
set distribution configuration {auto-topology | manual-general}
ip-version {ipv4 | ipv6 | all} ip-mask <Mask>
```

Parameters

Parameter	Notes
`auto-topology`	Configures the distribution mode to Auto-Topology (Per-Port).
`manual-general`	Configures the distribution mode to Manual General.
`ipv4`	Configures the distribution mode for IPv4 traffic only.
`ipv6`	Configures the distribution mode for IPv6 traffic only.
`all`	Configures the distribution mode for IPv4 and IPv6 traffic.

Parameter	Notes

`ip-mask <Mask>`	Must be the same as the distribution matrix size.
	Must be specified in the Hex format.
	Follow these steps:
	1. Examine the distribution matrix size:
	`> show distribution verification verbose`
	Examine the `Matrix Size` line.
	Example:
	`...`
	`Matrix Size 512`
	`...`
	2. Exit from the Gaia gClish to the Expert mode.
	3. Convert the matrix size from the decimal to the hexadecimal format:
	`printf '%x\n' <Matrix Size>`
	Example:
	`[Expert@MyChassis-ch0x-0x:0]# printf '%x\n' 512`
	`200`
	`[Expert@MyChassis-ch0x-0x:0]#`
	4. Go to the Gaia gClish:
	`gclish`
	5. Configure the distribution mode with the required mask:
	`> set distribution ... ip-mask <Matrix Size in HEX>`
	Example:
	`> set distribution ... ip-mask 200`

Configuring the Interface Distribution Mode (set distribution interface)

Description

Use these Gaia gClish commands on a Security Group to:

- Set the interface Distribution Mode - For an interface when the system is not working in the General Mode
- Show the interface Distribution Mode - If it is assigned by Auto-Topology, or is manually configured

Note - In VSX mode, you must go to the context of the applicable Virtual System before you can change the interface Distribution Mode.
Run the "`set virtual-system <VS ID>`" command.

Syntax to set the interface Distribution Mode

```
set distribution interface <Name of Interface> configuration {user
| network | policy}
```

Syntax to show the interface Distribution Mode

```
show distribution interface <Name of Interface> configuration
```

Parameters

Parameter	Description
<Name of Interface>	Interface name as assigned by the operating system.
`user`	Manually assign the **User** (**Internal**) Distribution Mode - based on the Destination IP address.
`network`	Manually assign the **Network** (**External**) Distribution Mode - based on the Source IP address.
`policy`	Use **Auto-Topology** to automatically assign the Distribution Mode according to the policy.

Examples

Example 1 - Set the Distribution Mode to Network (External)

```
[Global] MyChassis-ch01-01 > set distribution interface eth1-01
configuration network
/bin/distutil set_ifn_dist_mode eth1-01 external
```

Example 2 - Set the Distribution Mode to use the Auto-Topology to assign traffic according to the policy

```
[Global] MyChassis-ch01-01 > set distribution interface eth1-01
configuration policy
/bin/distutil set_ifn_dist_mode eth1-01 policy
```

Example 3 - Set the Distribution Mode to User (Internal)

```
[Global] MyChassis-ch01-01 > set distribution interface eth1-01
configuration user
/bin/distutil set_ifn_dist_mode eth1-01 internal
```

Showing Distribution Status (show distribution status)

Description

Use this Gaia gClish command on a Security Group to show the status report of the Distribution Mode.

Syntax

```
show distribution status [verbose]
```

Examples

Example 1 - Regular output

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> show distribution status
distribution:
  l4_mode: 'on'
  mode: general
matrix:
  actual_size: '512'
ports:
  eth1-05: policy-internal
  eth1-06: policy-internal
[Global] MyChassis-ch01-01>
```

Example 2 - Verbose output

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> show distribution verification verbose
Test:               Configuration:      Verification:       Result:
Mode                per-port            per-port            Passed
L4 Mode             on                  on                  Passed
Matrix Size         512                 512                 Passed
eth2-08             policy-external     policy-external     Passed
eth1-08             policy-internal     policy-internal     Passed
eth2-07             policy-internal     policy-internal     Passed
eth2-06             policy-internal     policy-internal     Passed
eth1-05             manual-internal     manual-internal     Passed
eth1-06             policy-internal     policy-internal     Passed
eth1-07             policy-internal     policy-internal     Passed

Verification passed successfully
[Global] MyChassis-ch01-01>
```

Explanation about the output

Field	Instructions
`l4_mode`	Shows the Layer 4 distribution status: ■ `on`- enabled ■ `off`- disabled
`mode`	Shows the currently configured Distribution Mode: ■ `per-port` - Auto-Topology ■ `user` - User (Internal) ■ `network` - Network (External) ■ `general` - General
`matrix` > `actual_size`	Shows the size of the Distribution Mode matrix.
`ports`	Shows the Distribution Mode assignment for each interface.

Running a Verification Test (show distribution verification)

Description

Use this Gaia gClish command on a Security Group to run a verification test of the Distribution Mode configuration.

This test compares the Security Group configuration with the actual results.

You can see a summary or a verbose report of the test results.

Syntax

```
show distribution verification [verbose]
```

Examples

Example 1- Verbose output of successful tests

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show distribution verification verbose
Test:               Configuration:      Verification:       Result:
Mode                per-port            per-port            Passed
L4 Mode             off                 off                 Passed
Matrix Size         512                 512                 Passed
eth2-16             policy-internal     policy-internal     Passed
eth1-16             policy-internal     policy-internal     Passed
eth1-15             policy-external     policy-external     Passed
[Global] MyChassis-ch01-01 >
```

Example 2 - Verbose output of failed tests

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show distribution verification verbose
Test:               Configuration:      Verification:       Result:
Mode                per-port            per-port            Passed
L4 Mode             on                  off                 Failed
Matrix Size         512                 0                   Failed
eth1-05             policy-internal     policy-internal     Passed
eth1-06             policy-internal     policy-internal     Passed
eth2-05             policy-external     policy-external     Passed
eth2-06             manual-internal     policy-external     Failed

Verification failed with above errors
[Global] MyChassis-ch01-01 >
```

Configuring the Layer 4 Distribution Mode and Masks (set distribution l4-mode)

Description

Use these commands in Gaia gClish on a Security Group to:

- Enable Layer 4 distribution and set new masks for the IP address and the port
- Disable Layer 4 distribution
- Show Layer 4 Distribution Mode and masks

Syntax

`set distribution l4-mode enabled`
`set distribution l4-mode disabled`
`show distribution l4-mode`

Examples

Example 1 - Configure the Layer 4 Distribution Mode

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> set distribution l4-mode enabled
1_01:
success

1_02:
success
[Global] MyChassis-ch01-01>
```

Example 2 - Disable the Layer 4 Distribution Mode

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> set distribution l4-mode disabled
1_01:
success

1_02:
success
[Global] MyChassis-ch01-01>
```

Example 3 - Show the current Layer 4 Distribution Mode

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> show distribution l4-mode
1_01:
L4 Distribution: Enabled

1_02:
L4 Distribution: Enabled
[Global] MyChassis-ch01-01>
```

Configuring the Cluster State (g_clusterXL_admin)

Description

Use the "`g_clusterXL_admin`" command in the Expert mode to change the cluster state manually, to UP or DOWN, for one or more Security Group Members.

Use Case

This command is useful for tests and debug.

Best Practice - Do **not** use this command in production environments, because it can cause performance degradation.

Syntax

```
g_clusterXL_admin -h
g_clusterXL_admin -b <SGM IDs> {up | down [-a]} [-r]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`up`	Changes the cluster state to UP.
`down`	Changes the cluster state to DOWN.
`-a`	Synchronizes accelerated connections to other Security Group Members.
`-r`	Runs this command on all `<SGM IDs>`, except the local Security Group Member.

Notes:

- When the Security Group Member is in the Administrative **DOWN** state:
  - Gaia gClish commands do not run on this Security Group Member.
  - Traffic is not sent to this Security Group Member.
  - The "`asg stat`" command shows this Security Group Member as "**DOWN (admin)**".
- When the cluster state of the Security Group Member is changed to Administrative **UP**, it automatically synchronizes the configuration from a different Security Group Member that is in the UP state.
- This command cannot change the state of a Security Group Member to **UP** if it is in the **DOWN** state because of a software or hardware problem.
- The "`g_clusterXL_admin`" command generates log entries.
  To see these log entries, run:

  ```
  asg log --file audit
  ```

Example

```
[Expert@MyChassis-ch0x-0x:0]# g_clusterXL_admin -b 2_03 up
You are about to perform blade_admin up on blades: 2_03
This action will change members state

Are you sure? (Y - yes, any other key - no) y

Blade_admin up requires auditing
Enter your full name: John Doe
Enter reason for blade_admin up [Maintenance]: test
WARNING: Blade_admin up on blades: 2_03, User: John Doe, Reason: test

Members outputs:
-*- 1 blade: 2_03 -*-
Setting member to normal operation ...
Member current state is ACTIVE
[Expert@MyChassis-ch0x-0x:0]#
```

Configuring a Unique MAC Identifier (asg_unique_mac_utility)

In This Section:

Background ... 173
Configuring the Unique MAC Identifier Manually ... 174
Options of the Unique MAC Identifier Utility ... 174

Background

When there are more than one Security Group on a Layer 2 segment, the Unique MAC Identifier must be different for each Security Group.

The Unique MAC Identifier is assigned by default during the initial setup.

The last octet of the management interface MAC address is the Unique MAC Identifier.

The last octet of the management interface MAC address is set for these data interface types:

- Interfaces with names in the "`eth`*`X`*`-`*`YZ`*" format
- Bond interfaces
- VSX`wrp` interfaces
- VLAN interfaces

If there is no configured management interface, the Unique MAC Identifier is assigned the default value 254.

Use the "`asg_unique_mac_utility`" command in Gaia gClish or the Expert mode to set:

- Data interface Unique MAC Identifier
- Host name

Configuring the Unique MAC Identifier Manually

Step	Instructions
1	Connect to the command line on the Security Group.
2	Run this command in Gaia gClish or the Expert mode: `asg_unique_mac_utility`

3	Select an option from the menu and follow the instructions on the screen.
	Example:
	`----------`
	`| Unique MAC Utility |`
	`----------`
	`| HOSTNAME [MySecurityGroup] |`
	`| Unique MAC [192] |`
	`----------`
	
	`Choose one of the following options:`
	`----------`
	`1) Set Hostname with Unique MAC wizard`
	`2) Apply Unique MAC from current HOSTNAME`
	`3) Manual set Unique MAC`
	`4) Exit`

4	Reboot the Security Group to apply the new Unique MAC Identifier: `reboot -b all`

Options of the Unique MAC Identifier Utility

The options for setting the Unique MAC Identifier are:

"Set Hostname with Unique MAC wizard"

The "`_asg`" suffix and the setup number, between 1 and 254, are added to the setup name.

Example:

Setup Name	Suffix	Setup number
`My_SG`	`_asg`	`22`

This creates a new host name with a Unique MAC Identifier of 22.

The setup number replaces the Unique MAC Identifier default value of 254.

New Host Name	Unique MAC Identifier
`My_SG_asg22`	`22`

After reboot, all data interface MAC addresses have the new Unique MAC Identifier value 16.

Example:

```
eth1-01 00:1C:7F:XY:ZW:16
```

Note - The last octet for `eth1-01`, shown in bold, is 16 hex (22 decimal).

"Apply Unique MAC from current Hostname"

Assign a new Unique MAC Identifier to the interfaces.

The new Unique MAC Identifier is created from the setup number in the host name.

The current host name must first comply with the setup name number convention:

```
/asg suffix/setup
```

"Manual set Unique MAC"

Set the Unique MAC Identifier to the default value of `254`.

Working with the ARP Table (asg_arp)

In This Section:

The 'asg_arp' Command ... 177
Example Default Output ... 179
Example Verbose Output ... 180
Example Output for Verifying MAC Addresses ... 180
Verifying ARP Entries ... 180
Example Legacy Output ... 181

The 'asg_arp' Command

Description

The `asg_arp` command in the Expert mode shows the ARP cache for the whole Security Group or for the specified Security Group Member, interface, MAC address, and Host name.

This command shows summary or verbose information.

Syntax

`asg_arp -h`
`asg_arp [-b <SGM IDs>] [-v] [--verify] [-i <Name of Interface>] [-m <MAC Address>] [<Hostname>]`
`asg_arp --legacy`

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-v`	Verbose mode that shows detailed Security Group Member cache information.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`-i <Name of Interface>`	Shows the ARP cache for the specified interface.
`-m <MAC Address>`	Shows the ARP cache for the specified MAC address.
`<Hostname>`	Shows the ARP cache for the specified host name.
`--verify`	Runs MAC address verification on all Maestro Sites and shows the results.
`--legacy`	Shows the ARP cache for each Security Group Member in the legacy format.

Example Default Output

This example shows the ARP cash in the Default Mode:

```
[Expert@MyChassis-ch0x-0x:0]# asg_arp
Address              HWaddress           Iface
172.23.19.4          54:7F:EE:6A:D0:BC   eth1-Mgmt2
1_01                 00:1C:7F:01:04:FE   Sync
1_2                  00:1C:7F:02:04:FE   Sync
ssm1                 02:02:03:04:05:40   eth1-CIN
ssm2                 04:02:03:04:05:40   eth2-CIN
[Expert@MyChassis-ch0x-0x:0]#
```

Example Verbose Output

This example shows the ARP cash in the Verbose Mode:

```
[Expert@MyChassis-ch0x-0x:0]# asg_arp -v
Address              HWtype   HWaddress           Flags Mask  Iface               SGMs
172.23.19.4          ether    54:7F:EE:6A:D0:BC   C           eth1-Mgmt2          1_01
1_01                 ether    00:1C:7F:01:04:FE   C           Sync                1_02
1_2                  ether    00:1C:7F:02:04:FE   C           Sync                1_01
ssm1                 ether    02:02:03:04:05:40   C           eth1-CIN            1_01,1_02
ssm2                 ether    04:02:03:04:05:40   C           eth2-CIN            1_01
[Expert@MyChassis-ch0x-0x:0]#
```

Example Output for Verifying MAC Addresses

This example shows the output of the MAC address verification (on a Single Chassis):

```
[Expert@MyChassis-ch0x-0x:0]# asg_arp --verify
Address              HWtype   HWaddress           Flags Mask  Iface               SGMs
172.23.19.4          ether    54:7F:EE:6A:D0:BC   C           eth1-Mgmt2          1_01
1_01                 ether    00:1C:7F:01:04:FE   C           Sync                1_02
1_2                  ether    00:1C:7F:02:04:FE   C           Sync                1_01
ssm1                 ether    02:02:03:04:05:40   C           eth1-CIN            1_01,1_02
ssm2                 ether    04:02:03:04:05:40   C           eth2-CIN            1_01

MAC address for IP 172.23.19.4 is inconsistent across the SGMs

------------------------------------------------------------------------------
Collecting information from SGMs...
------------------------------------------------------------------------------
Verifying FW1 mac magic value on all SGMs...
Success
------------------------------------------------------------------------------
Verifying IPV4 and IPV6 kernel values...
Success
------------------------------------------------------------------------------
Verifying FW1 mac magic value in /etc/smodb.json...
Success
------------------------------------------------------------------------------
Verifying MAC address on local chassis (Chassis 1)...
Success
------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Verifying ARP Entries

Use these commands to confirm that the Unique MAC value has changed.

For the Unique MAC database value, run this command in the Expert mode:

```
g_allc dbget chassis:private:magic_mac
```

Example:

```
[Expert@MyChassis-ch0x-0x:0]# g_allc dbget chassis:private:magic_mac
-*- 4 sgms: 1_01 1_02 2_02 2_03 -*-
22
```

For the Unique MAC Kernel value, run this command in Gaia gClish:

```
fw ctl get int fwha_mac_magic
```

Example:

```
[Global] MyChassis-ch01-01> fw ctl get int fwha_mac_magic
-*- 4 sgms: 1_01 1_02 2_02 2_03 -*-
fwha_mac_magic = 22
[Global] MyChassis-ch01-01>
```

You can display the magic attribute for interfaces of the type `eth`*X*`-`*YZ* with the "`ifconfig`" command in the Expert mode.

Example:

```
[Expert@MyChassis-ch0x-0x:0]# ifconfig eth1-01
eth1-01 Link encap:Ethernet HWaddr 00:1C:7F:81:01:16
          inet6 addr: fe80::21c:7fff:fe81:116/64 Scope:Link
          UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
          RX packets:154820 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0 RX bytes:15965660 (15.2 MiB)
          TX bytes:2003398 (1.9 MiB)
[Expert@MyChassis-ch0x-0x:0]#
```

Example Legacy Output

This example shows ARP cache for each Security Group Member in the Legacy Mode output:

```
[Expert@MyChassis-ch0x-0x:0]# asg_arp --legacy
1_01:
Address                  HWtype  HWaddress           Flags Mask            Iface
ssm2                     ether   04:02:03:04:05:40   C                     eth2-CIN
ssm1                     ether   02:02:03:04:05:40   C                     eth1-CIN
1_2                      ether   00:1C:7F:02:04:FE   C                     Sync
172.23.19.4              ether   54:7F:EE:6A:D0:BC   C                     eth1-Mgmt2
1_02:
Address                  HWtype  HWaddress           Flags Mask            Iface
1_01                     ether   00:1C:7F:01:04:FE   C                     Sync
ssm1                     ether   02:02:03:04:05:40   C                     eth1-CIN
[Expert@MyChassis-ch0x-0x:0]#
```

Working with the GARP Chunk Mechanism

In This Section:

Description 182
Configuration 183
Verification 184

Description

When Proxy ARP is enabled, the Firewall responds to ARP requests for hosts other than itself.

When failover occurs between Security Group Members, the new Active Security Group Member sends Gratuitous ARP (GARP) Requests with its own (new) MAC address to update the network ARP tables.

To prevent network congestion during failover, GARP Requests are sent in user defined groups called chunks.

Each chunk contains a predefined number of GARP Requests based on these parameters:

- The number of GARP Requests in each chunk (default is 1000 in each HTU).
- High Availability Time Unit (HTU) - the time interval (1 HTU = 0.1 sec), after which a chunk is sent.
- The chunk mechanism iterates on the proxy ARP IP addresses, and each time sends GARP Requests only for some of them until it completes the full list.

When the iteration sends the full list, it waits *N* HTUs and sends the list again.

Configuration

Important - To make the configuration permanent (to survive reboot), add the applicable kernel parameters to the `$FWDIR/boot/modules/fwkern.conf` file with this command:

```
g_update_conf_file fwkern.conf <Parameter>=<Value>
```

For example, to send 10 GARP Requests each second, set the value of the kernel parameter `fwha_refresh_arps_chunk` to 1:

```
g_fw ctl set int fwha_refresh_arps_chunk 1
```

To send 50 GARP Requests each second, set the value of the kernel parameter `fwha_refresh_arps_chunk` to 5:

```
g_fw ctl set int fwha_refresh_arps_chunk 5
```

Whenever the iteration is finished sending GARP Requests for the entire list, it waits *N* HTUs and sends the GARP Requests again.

The time between the iterations can be configured with these kernel parameters:

Kernel Parameter	Instructions
`fwha_periodic_send_garps_interval1`	The default value is 1 HTU (0.1 second). The Security Group sends the GARP immediately after failover. **Important** - Do not change this value.
`fwha_periodic_send_garps_interval2`	The default value is 10 HTUs (1 second). After the iteration sends the GARP list, it waits for this period of time and sends it again.
`fwha_periodic_send_garps_interval3`	The default value is 20 HTUs (2 seconds). After the iteration sends the GARP list, it waits for this period of time and sends it again.
`fwha_periodic_send_garps_interval4`	The default value is 50 HTUs (5 seconds). After the iteration sends the GARP list, it waits for this period of time and sends it again.
`fwha_periodic_send_garps_interval5`	The default value is 100 HTUs (10 seconds). After the iteration sends the GARP list, it waits for this period of time and sends it again.

To change an interval, run in the Expert mode:

```
g_fw ctl set int fwha_periodic_send_garps_interval<N> <Value>
```

To apply the intervals, run in the Expert mode:

```
g_fw ctl set int fwha_periodic_send_garps_apply_intervals 1
```

Verification

To send GARP Requests manually, on the SMO, run in the Expert mode:

```
g_fw ctl set int test_arp_refresh 1
```

This causes GARP Requests to be sent (same as was failover).

To debug, run in the Expert mode:

```
g_fw ctl zdebug -m cluster + ch_conf | grep fw_refresh_arp_proxy_
on_failover
```

NAT and the Correction Layer on a VSX Gateway

In a VSX Gateway, the guidelines in NAT and the Correction Layer on a Security Gateway apply to each Virtual System individually.

For best results, manage an entire session by a specified Virtual System on the same Security Group Member.

When a Virtual Switch (junction) connects several Virtual Systems, the same session can be handled by one Virtual System on one Security Group Member, and by another Virtual System on a different Security Group Member.

When a packet reaches a Virtual System from a junction, the system VSX Stateless Correction Layer checks the distribution again according to the Distribution Mode configured on the WRP interface. It can decide to forward the packet to a different Security Group Member.

In addition, on each Virtual System, the stateful Correction Layer can forward session packets, similar to the Security Gateway.

All forwarding operations have a performance impact. Therefore, the Distribution Mode configuration should minimize forwarding operations.

To achieve optimal distribution between Security Group Members in a Security Group in VSX mode:

NAT Rules	Guidelines
Not using NAT rules on any Virtual System	Set the Distribution Mode to **General**.
Using NAT rule on at least one Virtual System	■ On the Virtual Systems that use NAT rules: • Set the Distribution Mode to **User** for the networks hidden behind NAT. • Set the Distribution Mode to **Network** for the destination networks. ■ On the remaining Virtual Systems that do not use NAT rules: • Set the Distribution Mode to **User** for the internal networks. • Set the Distribution Mode to **Network** for the external networks.

NAT and the Correction Layer on a Security Gateway

For optimal system performance, one Security Group Member handles all traffic for a session.

With NAT, packets sent from the client to the server can be distributed to a different Security Group Member than packets from the same session sent from the server to the client.

The system Correction Layer must then forward the packet to the correct Security Group Member.

Configuring the Distribution Mode correctly keeps correction situations to a minimum and optimizes system performance.

To achieve optimal distribution between Security Group Members in a Security Group in Gateway mode:

NAT Rules	Guidelines
Not using NAT rules	Set the Distribution Mode to **General**.
Using NAT rule	■ Set the Distribution Mode to **User** for the networks hidden behind NAT. ■ Set the Distribution Mode to **Network** for the destination networks.

IPS Management During a Cluster Failover

You can configure how IPS is managed during a cluster failover.

This occurs when one Cluster Member takes over for a different Cluster Member to provide High Availability.

You must run this command in the Expert mode.

Syntax to configure the IPS behavior during a cluster failover

```
asg_ips_failover_behavior {connectivity | security}
```

Parameters

Parameter	Description
`connectivity`	Prefers connectivity (default). Keeps connections alive, even if IPS inspection cannot be guaranteed.
`security`	Prefers security. Closes connections, for which IPS inspection cannot be guaranteed.

Syntax to view the configured IPS behavior during a cluster failover

```
fw ctl get int fwha_ips_reject_on_failover
```

Explanation:

Output	Current Configuration
`fwha_ips_reject_on_failover = 0`	Prefers connectivity
`fwha_ips_reject_on_failover = 1`	Prefers security

IPv6 Neighbor Discovery

Neighbor discovery works over the ICMPv6 Neighbor Discovery protocol, which is the functional equivalent of the IPv4 ARP protocol.

ICMPv6 Neighbor Discovery Protocol must be explicitly permitted in the Access Control Rule Base for all bridged networks.

This is different from ARP. ARP traffic is Layer 2 only, therefore it permitted regardless of the Rule Base.

This is an example of an explicit Rule Base that permits ICMPv6 Neighbor Discovery protocol:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
IPv6 Neighbor Discovery	Network object that represents the Bridged Network	Network object that represents the Bridged Network	Any	neighbor-advertisement neighbor-solicitation router-advertisement router-solicitation redirect6	Accept	Log	Policy Targets

Logging and Monitoring

This section provides instructions for monitoring the environment.

CPView

Overview of CPView

Description

CPView is a text based built-in utility on a Check Point computer.

CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Group).

The CPView continuously updates the data in easy to access views.

On Security Group, you can use this statistical data to monitor the performance.

For more information, see sk101878.

Syntax

```
cpview --help
```

CPView User Interface

The CPView user interface has three sections:

Section	Description
Header	This view shows the time the statistics in the third view are collected. It updates when you refresh the statistics.
Navigation	This menu bar is interactive. Move between menus with the arrow keys and mouse. A menu can have sub-menus and they show under the menu bar.
View	This view shows the statistics collected in that view. These statistics update at the refresh rate.

Using CPView

Use these keys to navigate the CPView:

Key	Description
Arrow keys	Moves between menus and views. Scrolls in a view.
Home	Returns to the **Overview** view.
Enter	Changes to the **View Mode**. On a menu with sub-menus, the **Enter** key moves you to the lowest level sub-menu.
Esc	Returns to the **Menu Mode**.
Q	Quits CPView.

Use these keys to change CPView interface options:

Key	Description
R	Opens a window where you can change the refresh rate. The default refresh rate is 2 seconds.
W	Changes between wide and normal display modes. In wide mode, CPView fits the screen horizontally.
S	Manually sets the number of rows or columns.
M	Switches on/off the mouse.
P	Pauses and resumes the collection of statistics.

Use these keys to save statistics, show help, and refresh statistics:

Key	Description
C	Saves the current page to a file. The file name format is: `cpview_<ID of the cpview process>.cap<Number of the capture>`
H	Shows a tooltip with CPView options.
Space bar	Immediately refreshes the statistics.

Network Monitoring

You can monitor and log traffic.

Working with Interface Status (asg if)

Description

Use the "`asg if`" command in Gaia gClish or the Expert mode to:

- Enable and disable the interfaces
- Show information about interfaces:
  - IPv4, IPv6, and MAC address
  - Interface type
  - Link State
  - Speed
  - MTU
  - Duplex

Syntax

`asg if -h`
`asg if -i <`*`Interface1`*`>[,<`*`Interface2`*`>,...,<`*`InterfaceN`*`>] [-v] [{enable | disable}]`
`asg if -ip <`*`IP Address`*`>`

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows information about all interfaces.
`-i <Interface1> [,<Interface2>,...,<InterfaceN>]`	Shows information only about the interfaces specified by their names. ■ You can specify one or more interfaces. ■ If you specify more than interface, you must separate their names by a comma without spaces. Example: `asg if -i Sync,eth1-Mgmt1`
`-v`	Shows verbose output. **Note** - This view is not supported for logical interfaces (for example, Bond, VLAN, and `ethX-MgmtY` interfaces).
`enable`	Enables the specified interfaces.
`disable`	Disables the specified interfaces.
`-ip <IP Address>`	Shows information only about one interface specified by its IPv4 or IPv6 address.

Verbose Mode (asg if -v)

The Verbose Mode shows extended information, including information retrieved from the switch.

You can use the Verbose Mode for one interface or a comma-separated list of interfaces (without spaces).

This operation can take a few seconds for each interface.

Example output

```
[Expert@MyChassis-ch0x-0x:0]# asg if -i eth1-01 -v
Collecting information, may take few seconds
+-------------------------------------------------------------------------------------------+
|Interfaces Data                                                                            |
+-------------------------------------------------------------------------------------------+
|Interface|IPv4 Address         |Info        |State          |Speed   |MTU       |Duplex  |
|         |MAC  Address         |            |(ch1)/(ch2)    |        |          |        |
|         |IPv6 Address (global)|            |               |        |          |        |
|         |IPv6 Address (local) |            |               |        |          |        |
+---------+---------------------+------------+---------------+--------+----------+--------+
|eth1-01  |-                    |Bond slave  |(up)/(up)      |10G     |1500      |Full    |
|         |00:1c:7f:a1:01:0     |            |master:        |        |          |        |
|         |-                    |            |bond1(up)/(up)|        |          |        |
|         |-                    |            |               |        |          |        |
+---------+---------------------+------------+---------------+--------+----------+--------+
|Comment                                                                                    |
+-------------------------------------------------------------------------------------------+
|internal interface                                                                         |
+-------------------------------------------------------------------------------------------+
|Traffic                                                                                    |
+-------------------------------------------------------------------------------------------+
|media            |In traffic |In pkt(uni/mul/brd)|Out traffic    |Out pkt(uni/mul/brd)   |
+-----------------+-----------+-------------------+---------------+-----------------------+
|FTLF8528P2BNV-EM |28.8Kbps   |0pps/38pps/5pps    |4.1Mbps        |0pps/355pps/0pps       |
+-------------------------------------------------------------------------------------------+
|Errors (total/pps)                                                                         |
+-------------------------------------------------------------------------------------------+
|OutDiscards                  |InDiscards         |InErrors       |OutErrors              |
+-----------------------------+-------------------+---------------+-----------------------+
|0/0                          |0/0                |0/0            |0/0                    |
+-----------------------------+-------------------+---------------+-----------------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Global View of All Interfaces (show interfaces)

Use the "`show interfaces`" command in Gaia gClish to show the current status of all defined interfaces on the system.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> show interfaces
+-------------------------------------------------------------------------------------------+
|Interfaces Data                                                                            |
+-------------------------------------------------------------------------------------------+
|Interface  |IPv4 Address      |Info        |State        |Speed    |MTU       |Duplex  |
|           |MAC  Address      |            |(ch1)        |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|bond1      |17.17.17.10       |Bond Master |(down)       |NA       |NA        |NA      |
|           |00:1c:7f:81:05:fe |            |slaves:      |         |          |        |
|           |                  |            |eth1-05(down)|         |          |        |
|           |                  |            |eth2-05(down)|         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|  eth1-05  |-                 |Bond slave  |(down)       |10G      |1500      |Full    |
|           |00:1c:7f:81:05:fe |            |master:      |         |          |        |
|           |                  |            |bond1(down)  |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|  eth2-05  |-                 |Bond slave  |(down)       |10G      |1500      |Full    |
|           |00:1c:7f:81:05:fe |            |master:      |         |          |        |
|           |                  |            |bond1(down)  |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|bond1.201  |18.18.18.10       |Vlan        |(down)       |NA       |NA        |NA      |
|           |00:1c:7f:81:05:fe |            |             |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|br0        |-                 |Bridge Mast |(up)         |NA       |NA        |NA      |
|           |00:1c:7f:81:07:fe |            |ports:       |         |          |        |
|           |                  |            |eth2-07(down)|         |          |        |
|           |                  |            |eth1-07(down)|         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|  eth1-07  |-                 |Bridge port |(down)       |10G      |1500      |Full    |
|           |00:1c:7f:81:07:fe |            |master:      |         |          |        |
|           |                  |            |br0(up)      |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|  eth2-07  |-                 |Bridge port |(down)       |10G      |1500      |Full    |
|           |00:1c:7f:82:07:fe |            |master:      |         |          |        |
|           |                  |            |br0(up)      |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|eth1-01    |15.15.15.10       |Ethernet    |(up)         |10G      |1500      |Full    |
|           |00:1c:7f:81:01:fe |            |             |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|eth1-Mgmt4 |172.23.9.67       |Ethernet    |(up)         |10G      |1500      |Full    |
|           |00:d0:c9:ca:c7:fa |            |             |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|eth2-01    |25.25.25.10       |Ethernet    |(up)         |10G      |1500      |Full    |
|           |00:1c:7f:82:01:fe |            |             |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
|Sync       |192.0.2.1         |Ethernet    |(up)         |10G      |1500      |Full    |
|           |00:1c:7f:01:04:fe |            |             |         |          |        |
+-----------+------------------+------------+-------------+---------+----------+--------+
[Global] MyChassis-ch01-01>
```

Notes:

- This sample output shows that this Sync interface is a Bond-Master and if the interfaces are UP or DOWN.
- To add a comment to an interface, run in Gaia gClish:

  ```
  > set interface <Name of Interface> comment "<Comment Text>"
  ```

Monitoring Bond Interfaces (asg_bond)

In This Section:

Description

Use the "`asg_bond`" command in Gaia gClish or the Expert mode to show bond interfaces and to run these LACP packet tests:

- Test for MAC address consistency for each Security Group Member
- Test for bond slave state consistency for all Security Group Members
- Test for database consistency for all Security Group Members
- Confirm that the LACP aggregator IDs between bond interface and its slaves are compatible
- Confirm that the LACP packets pass between neighbors
- Compare the LACP packet keys between neighbors

You can run this command for specified bond interfaces or for all bond interfaces.

Syntax

```
asg_bond {-h | --help}
asg_bond [-v] [ -i <Filter>]
```

Parameters

Parameter	Instructions
`-h` `--help`	Shows the built-in help.
`-i` `<Filter>`	Filters the output for the bond interface specified by its complete or partial name.
`-v`	Runs LACP packet test for the specified bond interfaces.

Viewing a Global List of All Bond Interfaces (asg_bond)

Use the "`asg_bond`" command in Gaia gClish or the Expert mode without parameters to show all bond interfaces.

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_bond
+------+-----------------------------------------+---------+--------+------------------+
|Name  |Address                  |Mode           |Slaves   |Result  |Comments          |
+------+-------------------------+---------------+---------+--------+------------------+
|bond1 |(MAC)  00:1c:7f:81:02:fe|LACP 802.3ad   |eth1-02  |OK      |                  |
|      |(IPv4) 13.13.1.10       |Load Sharing   |eth1-03  |        |                  |
|      |                        |               |eth2-03  |        |                  |
|      |                        |               |eth2-02  |        |                  |
+------+-------------------------+---------------+---------+--------+------------------+
|bond3 |(MAC)  00:1c:7f:82:04:fe|XOR            |eth2-04  |OK      |                  |
|      |(IPv4) 23.23.1.10       |Load Sharing   |eth1-04  |        |                  |
+------+-------------------------+---------------+---------+--------+------------------+
|bond5 |(MAC)  00:1c:7f:81:07:fe|Round-Rubin    |eth1-07  |OK      |                  |
|      |(IPv4) 33.33.1.10       |Load Sharing   |eth2-07  |        |                  |
+------+-------------------------+---------------+---------+--------+------------------+
|bond7 |(MAC)  00:00:00:00:00:fe|Active-Backup  |         |OK      |- No slaves exist |
|      |                        |High Availability |      |        |                  |
+------+-------------------------+---------------+---------+--------+------------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Viewing a Specific Bond Interface (asg_bond -i)

Use the "`asg_bond -i <bond`*X*`>`" command in Gaia gClish or the Expert mode to show a specific bond interface.

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_bond -i bond5
+--------+-------------------------------+--------------+---------+--------+---------+
|Name    |Address                        |Mode          |Slaves   |Result  |Comments |
+--------+-------------------------------+--------------+---------+--------+---------+
|bond5   |(MAC)  00:1c:7f:81:07:fe       |Round-Rubin   |eth1-07  |OK      |         |
|        |(IPv4) 33.33.1.10              |Load Sharing  |eth2-07  |        |         |
+--------+-------------------------------+--------------+---------+--------+---------+
[Expert@MyChassis-ch0x-0x:0]#
```

Running a Bond Verification Test (asg_bond -v)

Use the "`asg_bond -v`" command in Gaia gClish or the Expert mode to run a bond verification test on all bond interfaces.

Example

This example shows the verification test results for all bond interfaces, including one with an error.

Notes:

- The comments column shows a description of problems detected by the verification tests.
- The interface `bond7` shows an incomplete definition with no slaves configured.

```
[Expert@MyChassis-ch0x-0x:0]# asg_bond -v
Listening for LACP packets [.............................]   [ OK ]

+-----+-----------------------+----------------+-------+------+-------------------------+
|Name |Address                |Mode            |Slaves |Result|Comments                 |
+-----+-----------------------+----------------+-------+------+-------------------------+
|bond1|(MAC) 00:1c:7f:81:02:fe |LACP 802.3ad    |eth1-02|Failed|eth1-02 missing LACP pkts|
|     |(IPv4)13.13.1.10       |Load Sharing    |eth1-03|      |eth1-03 missing LACP pkts|
|     |                       |                |eth2-03|      |eth2-03 missing LACP pkts|
|     |                       |                |eth2-02|      |eth2-02 missing LACP pkts|
+-----+-----------------------+----------------+-------+------+-------------------------+
|bond3|(MAC)  00:1c:7f:82:04:fe|XOR             |eth2-04|OK    |                         |
|     |(IPv4) 23.23.1.10      |Load Sharing    |eth1-04|      |                         |
+-----+-----------------------+----------------+-------+------+-------------------------+
|bond5|(MAC)  00:1c:7f:81:07:fe|Round-Rubin     |eth1-07|OK    |                         |
|     |(IPv4) 33.33.1.10      |Load Sharing    |eth2-07|      |                         |
+-----+-----------------------+----------------+-------+------+-------------------------+
|bond7|(MAC)  00:00:00:00:00:fe|Active-Backup   |       |OK    | - No slaves exist       |
|     |                       |High Availability|       |      |                         |
+-----+-----------------------+----------------+-------+------+-------------------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Monitoring Traffic (asg_ifconfig)

In This Section:

Description

The "`asg_ifconfig`" command in Gaia gClish or the Expert mode collects traffic statistics from all or a specified range of Security Group Members.

The combined output shows the traffic distribution between Security Group Members and their interfaces (calculated during a certain period).

The "`asg_ifconfig`" command has these modes:

Mode	Instructions
Native	This is the default setting. When you do not specify the "`analyze`" or "`banalyze`" option in the syntax, the command behaves almost in the same as the native Linux "`ifconfig`" command. However, the output shows statistics for all interfaces on all Security Group Members, and for interfaces on the local Security Group Member.
Analyze	Shows accumulated traffic information and traffic distribution between Security Group Members.
Banalyze	Shows accumulated traffic information and traffic distribution between interfaces.

Notes:

- The parameters "`analyze`" and "`banalyze`" are mutually exclusive.
  You cannot specify them in the same command.
- If you run this command in the context of a Virtual System, you can only see the output that applies to that context.

Syntax

```
asg_ifconfig -h
```

```
asg_ifconfig [-b <SGM IDs>] [<Name of Interface>] [analyze [-d <Delay>] [-a] [-v]]
```

```
asg_ifconfig [-b <SGM IDs>] [<Name of Interface>] [banalyze [-d <Delay>] [-a] [-v] [-rb] [-rd] [-rp] [-tb] [-td] [-tp]]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`<Name of Interface>`	Specifies the name of the interface.
`analyze`	Shows accumulated traffic information and traffic distribution between the Security Group Members. Use the "`-a`", "`-v`", and "`-d <Delay>`" parameters to show traffic distribution between interfaces.

Parameter	Description

`banalyze`	Shows accumulated traffic information and traffic distribution between the interfaces.
	Use the "`-a`", "`-v`", and "`-d <Delay>`" parameters to show traffic distribution between interfaces.
	By default, the traffic distribution table is not sorted.
	You can use these parameters to sort the traffic distribution table:
	■ `-rb` - Sort the output by the number of received (RX) bytes
	■ `-rd` - Sort the output by the number of received (RX) dropped packets
	■ `-rp` - Sort the output by the number of received (RX) packets
	■ `-tb` - Sort the output by the number of transmitted (TX) bytes
	■ `-td` - Sort the output by the number of transmitted (TX) dropped packets
	■ `-tp` - Sort the output by the number of transmitted (TX) packets
	For example, if you sort with the "`-rb`" option, the higher values appear at the top of the "`RX bytes`" column:
	`SGM ID  RX packets  RX bytes  RX dropped`
	`1_03  70%`
	`1_02  20%`
	`1_01  10%`

`-d <Delay>`	Delay, in seconds, between data samples. Default: 5 seconds.
`-a`	Shows total traffic volume. By default (without "`-a`"), the output shows the average traffic volume per second.
`-v`	Verbose mode. Shows detailed information of each interface and the accumulated traffic information

Examples

Example 1 - Default output

This example shows the total traffic sent and received by the interface `eth2-01` for all Security Group Members on Site 1 (Active Site)..

By default, the output shows the average traffic volume per second.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg_ifconfig -b chassis1 eth2-01

as1_02:
eth2-01     Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX packets:94 errors:0 dropped:0 overruns:0 frame:0
            TX packets:63447 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:5305 (5.1 KiB)  TX bytes:5688078 (5.4 MiB)

1_03:
eth2-01     Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX packets:137 errors:0 dropped:0 overruns:0 frame:0
            TX packets:26336 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:7591 (7.4 KiB)  TX bytes:2355386 (2.2 MiB)

1_04:
eth2-01     Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX packets:124 errors:0 dropped:0 overruns:0 frame:0
            TX packets:3098 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:6897 (6.7 KiB)  TX bytes:378990 (370.1 KiB)

1_05:
eth2-01     Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500 Metric:1
            RX packets:79 errors:0 dropped:0 overruns:0 frame:0
            TX packets:26370 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:4507 (4.4 KiB)  TX bytes:2216546 (2.1 MiB)
[Global] MyChassis-ch01-01>
```

Example 2 - The 'analyze' mode

This example shows:

- The accumulated and detailed traffic volume statistics for the interface `eth2-Sync` for each Security Group Member.
- The total for all Security Group Members.
- The traffic distribution for each Security Group Member.
- The "`-a`" option shows the total traffic volume instead of the average volume per second.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg_ifconfig eth2-Sync analyze -v -a
Command is executed on SGMs: chassis_active

1_01:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:01:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:225018 bytes:36970520 (37.0 MiB)  dropped:0
            TX: packets:3522445 bytes:1381032583 (1.4 GiB)  dropped:0

1_02:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:02:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:221395 bytes:35947248 (35.9 MiB)  dropped:0
            TX: packets:4674143 bytes:1850315554 (1.9 GiB)  dropped:0

1_03:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:03:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:10 bytes:644 (644.0 b)  dropped:0
            TX: packets:67826313 bytes:7345458105 (7.3 GiB)  dropped:0

1_04:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:04:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:13 bytes:860 (860.0 b)  dropped:0
            TX: packets:68489217 bytes:7487476060 (7.5 GiB)  dropped:0

1_05:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:05:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:203386 bytes:19214238 (19.2 MiB)  dropped:0
            TX: packets:7164109 bytes:2740761091 (2.7 GiB)  dropped:0

=*= Accumulative =*=
eth2-Sync   Link encap:Ethernet
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:649822 bytes:92133510 (92.1 MiB)  dropped:0
            TX: packets:151676227 bytes:20805043393 (20.8 GiB)  dropped:0

=*= Traffic Distribution =*=

-------------------------------------------------------------------------------
     SGM ID RX packets   RX bytes RX dropped TX packets   TX bytes TX dropped
-------------------------------------------------------------------------------
       1_01      34.6%      40.1%       0.0%       2.3%       6.6%       0.0%
       1_02      34.1%      39.0%       0.0%       3.1%       8.9%       0.0%
       1_03       0.0%       0.0%       0.0%      44.7%      35.3%       0.0%
       1_04       0.0%       0.0%       0.0%      45.2%      36.0%       0.0%
       1_05      31.3%      20.9%       0.0%       4.7%      13.2%       0.0%
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01>
```

Example 2 - The 'banalyze' mode

This example shows:

- The accumulated and detailed traffic volume statistics for the interface `eth2-Sync` on each Security Group Member.
- The total on each Security Group Member.
- The traffic distribution on each Security Group Member.
- The "`-a`" option shows the total traffic volume instead of the average volume per second.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg_ifconfig eth2-Sync banalyze -v -a
Command is executed on SGMs: chassis_active

1_01:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:01:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:225018 bytes:36970520 (37.0 MiB)  dropped:0
            TX: packets:3522445 bytes:1381032583 (1.4 GiB)  dropped:0

=*= Accumulative =*=
            RX: packets:225018 bytes:36970520 (37.0 MiB)  dropped:0
            TX: packets:3522445 bytes:1381032583 (1.4 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

1_02:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:02:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:221395 bytes:35947248 (35.9 MiB)  dropped:0
            TX: packets:4674143 bytes:1850315554 (1.9 GiB)  dropped:0

=*= Accumulative =*=
            RX: packets:221395 bytes:35947248 (35.9 MiB)  dropped:0
            TX: packets:4674143 bytes:1850315554 (1.9 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

1_03:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:03:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:10 bytes:644 (644.0 b)  dropped:0
            TX: packets:67826313 bytes:7345458105 (7.3 GiB)  dropped:0

=*= Accumulative =*=
            RX: packets:10 bytes:644 (644.0 b)  dropped:0
            TX: packets:67826313 bytes:7345458105 (7.3 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

1_04:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:04:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:13 bytes:860 (860.0 b)  dropped:0
            TX: packets:68489217 bytes:7487476060 (7.5 GiB)  dropped:0

=*= Accumulative =*=
            RX: packets:13 bytes:860 (860.0 b)  dropped:0
            TX: packets:68489217 bytes:7487476060 (7.5 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
```

```
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

1_05:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:05:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:203386 bytes:19214238 (19.2 MiB)  dropped:0
            TX: packets:7164109 bytes:2740761091 (2.7 GiB)  dropped:0

=*= Accumulative =*=
            RX: packets:203386 bytes:19214238 (19.2 MiB)  dropped:0
            TX: packets:7164109 bytes:2740761091 (2.7 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

=*= All Blades =*=
      RX: packets:649822 bytes:92133510 (92.1 MiB)  dropped:0
      TX: packets:148153782 bytes:20805043393(20.8 GiB)  dropped:0

=*= Traffic Distribution =*= (all blades)

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------
[Global] MyChassis-ch01-01>
```

Monitoring Multicast Traffic

In This Section:

Use these commands to show information about multicast traffic.

Showing Multicast Routing (asg_mroute)

Description

The "`asg_mroute`" command in Gaia gClish or the Expert mode shows this multicast routing information in a tabular format:

- **Source** - Source IP address
- **Dest** - Destination address
- **Iif** - Source interface
- **Oif** - Outbound interface

You can filter the output for specified interfaces and Security Group Members.

Syntax

```
asg_mroute -h
```

```
asg_mroute [-d <Destination Route>] [-s <Source Route>] [-i
<Source Interface>][-b <SGM IDs>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows all routes, interfaces and Security Group Members.
`-d <Destination Route>`	Specifies the destination multicast group IP address.
`-s <Source Route>`	Specifies the source IP address.
`-i <Source Interface>`	Specifies the source interface name.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)

Examples

Example 1 - Shows all multicast routes for all interfaces and Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg_mroute
+-------------------------------------------------------------------------------+
|Multicast Routing (All SGMs)                                                   |
+-------------------------------------------------------------------------------+
|Source                  |Dest                   |Iif            |Oif            |
+------------------------+-----------------------+---------------+---------------+
|12.12.12.1              |225.0.90.90            |eth1-01        |eth1-02        |
+------------------------+-----------------------+---------------+---------------+
|22.22.22.1              |225.0.90.90            |eth1-02        |eth1-01        |
+------------------------+-----------------------+---------------+---------------+
|22.22.22.1              |225.0.90.91            |eth1-02        |eth1-01        |
+------------------------+-----------------------+---------------+---------------+
[Global] MyChassis-ch01-01>
```

Example 2 - Shows only specific IP address, interfaces, destination IP address, or Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# asg_mroute -s 22.22.22.1 -i eth1-02 -d 225.0.90.91
+-------------------------------------------------------------------------------+
|Multicast Routing (All SGMs)                                                   |
+-------------------------------------------------------------------------------+
|Source                  |Dest                   |Iif            |Oif            |
+------------------------+-----------------------+---------------+---------------+
|22.22.22.1              |225.0.90.91            |eth1-02        |eth2-01        |
+------------------------+-----------------------+---------------+---------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Showing PIM Information (asg_pim)

Description

The `asg_pim` command in Gaia gClish or the Expert mode shows this PIM information in a tabular format:

- **Source** - Source IP address
- **Dest** - Destination IP address
- **Mode** - Both Dense Mode and Sparse Mode are supported
- **Flags** - Local source and MFC state indicators
- **In. intf** - Source interface
- **RPF** - Reverse Path Forwarding indicator
- **Out int** - Outbound interface
- **State** - Outbound interface state

You can filter the output for specified interfaces and Security Group Members.

Syntax

```
asg_pim -h
asg_pim [-b <SGM IDs>] [-i <if>]
asg_pim neighbors [-n <neighbor>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows all routes, interfaces and Security Group Members.

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`-i <if>`	Shows only the specified source interface.
`neighbors`	Runs verification tests to make sure that PIM `neighbors` are the same on all Security Group Members and shows this information: ■ **Verification** - Results of verification test ■ **Neighbor** - PIM neighbor ■ **Interface** - Interface name ■ **Holdtime** - Time in seconds to hold a connection open during peer negotiation ■ **Expires** - Minimum and Maximum expiration values for all Security Group Members
`-n <neighbor>`	Shows only the specified PIM `neighbor`.

Examples

Example 1 - Shows PIM information and multicast routes for all interfaces and Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg_pim
+-------------------------------------------------------------------------------------+
|PIM (All SGMs)                                                                       |
+-------------------------------------------------------------------------------------+
|source     |dest        |Mode      |Flags|In. intf |RPF       |Out. intf   |State     |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|12.12.12.1 |225.0.90.90 |Dense-Mode|L|M  |eth1-01  |none      |            |          |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.90 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.91 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
|           |            |          |     |         |          |eth2-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
Flags: L - Local source, M - MFC State
[Global] MyChassis-ch01-01>
```

Example 2 - Shows PIM Information for the specific interface on all Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# asg_pim -i eth1-02 -b all
+-------------------------------------------------------------------------------------+
|PIM (All SGMs)                                                                       |
+-------------------------------------------------------------------------------------+
|SGM 1_01                                                                             |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|source     |dest        |Mode      |Flags|In. intf |RPF       |Out. intf   |State     |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.90 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.91 |Dense-Mode|L    |eth1-02  |none      |eth1-01     |Forwarding|
|           |            |          |     |         |          |eth2-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
|SGM 1_02                                                                             |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|source     |dest        |Mode      |Flags|In. intf |RPF       |Out. intf   |State     |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.90 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.91 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
|           |            |          |     |         |          |eth2-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
[Expert@MyChassis-ch0x-0x:0]#
```

Example 3 - Shows PIM neighbors

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg_pim neighbors
+-------------------------------------------------------------------------------------+
|PIM Neighbors (All SGMs)                                                             |
+-------------------------------------------------------------------------------------+
|Verification:                                                                        |
|Neighbors Verification: Passed - Neighbors are identical on all blades               |
+--------------------+--------------------+--------------------+----------------------+
|Neighbor            |Interface           |Holdtime            |Expires(min-max)      |
+--------------------+--------------------+--------------------+----------------------+
|11.1.1.1            |bond1               |105                 |11:36:45-11:37:59     |
+--------------------+--------------------+--------------------+----------------------+
[Global] MyChassis-ch01-01>
```

Showing IGMP Information (asg_igmp)

Description

Use the `asg_igmp` command in Gaia gClish or the Expert mode to show IGMP information in a tabular format.

You can filter the output for specified interfaces and Security Group Members. If no Security Group Member is specified, the command runs a verification to make sure that IGMP data is the same on all Security Group Members:

- Group verification - Confirms the groups exist on all Security Group Members. If a group is missing on some Security Group Members, a message shows which group is missing on which blade.
- Global properties - Confirms the flags, address and other information are the same on all Security Group Members.
- Interfaces - Confirms that all blades have the same interfaces and that they are in the same state (UP or DOWN). If inconsistencies are detected, a warning message shows.

Syntax

```
asg_igmp -h
```

```
asg_igmp [-i <interface>] [-b <SGM IDs>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-i <interface>`	Source interface name.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)

Examples

Example 1 - Shows IGMP information and multicast routes for all interfaces and Security Group Members

Note - In this example, the verification detected an interface inconsistency.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg_igmp

Collecting IGMP information, may take few seconds...
+-------------------------------------------------------------------------------------------+
|IGMP (All SGMs)                                                                            |
+-------------------------------------------------------------------------------------------+
|Interface: eth1-01
+-------------------------------------------------------------------------------------------+
|Verification:                                                                              |
|Group Verification: Passed - Information is identical on all blades                        |
|Global Properties Verification: Passed - Information is identical on all blades            |
+-------------------------------------------------------------------------------------------+
|Group               |Age       |Expire                                                     |
+--------------------+----------+-----------------------------------------------------------+
|225.0.90.91         |2m        |4m                                                         |
+--------------------+----------+-----------------------------------------------------------+
|Flags     |IGMP Ver |Query Interval |Query Response Interval  |protocol |Advertise Address|
+----------+---------+---------------+-------------------------+---------+-----------------+
|Querier   |2        |125            |10                       |PIM      |12.12.12.10      |
+-------------------------------------------------------------------------------------------+

+-------------------------------------------------------------------------------------------+
|Interface: eth1-02                                                                         |
+-------------------------------------------------------------------------------------------+
|Verification:                                                                              |
|Group Verification: Failed - Found inconsistency between blades                            |
| -Group 225.0.90.92: missing in blades 1_02                                                |
|Global Properties Verification: Passed - Information is identical on all blades            |
+-------------------------------------------------------------------------------------------+
|Group               |Age       |Expire                                                     |
+--------------------+----------+-----------------------------------------------------------+
|225.0.90.92         |2m        |3m                                                         |
+--------------------+----------+-----------------------------------------------------------+
|Flags     |IGMP Ver |Query Interval |Query Response Interval  |protocol |Advertise Address|
+----------+---------+---------------+-------------------------+---------+-----------------+
|Querier   |2        |125            |10                       |PIM      |22.22.22.10      |
+-------------------------------------------------------------------------------------------+

+-------------------------------------------------------------------------------------------+
|Interface: eth2-01                                                                         |
+-------------------------------------------------------------------------------------------+
|Verification:                                                                              |
|Group Verification: Passed - Information is identical on all blades                        |
|Global Properties Verification: Passed - Information is identical on all blades            |
+-------------------------------------------------------------------------------------------+
|Group               |Age       |Expire                                                     |
+--------------------+----------+-----------------------------------------------------------+
|225.0.90.90         |2m        |3m                                                         |
+--------------------+----------+-----------------------------------------------------------+
|Flags     |IGMP Ver |Query Interval |Query Response Interval  |protocol |Advertise Address|
+----------+---------+---------------+-------------------------+---------+-----------------+
|Querier   |2        |125            |10                       |PIM      |2.2.2.10         |
+-------------------------------------------------------------------------------------------

NOTE: Inconsistency found in interfaces configuration between blades
Inconsistent interfaces: eth1-02
[Global] MyChassis-ch01-01>
```

Example 2 - Shows IGMP Information for a specified interface

```
[Expert@MyChassis-ch0x-0x:0]# asg_igmp -i bond1.3
Collecting IGMP information, may take few seconds...
+-------------------------------------------------------------------------------------------------+
|IGMP (All SGMs)                                                                                  |
+-------------------------------------------------------------------------------------------------+
|Interface: bond1.3                                                                               |
+-------------------------------------------------------------------------------------------------+
|Verification                                                                                     |
|Group Verification: Passed - Information is identical on all blades                              |
|Global Properties Verification: Passed - Information is identical on all blades                  |
+-------------------------------------------------------------------------------------------------+
|Group               |Age       |Expire                                                           |
--------------------+----------+-----------------------------------------------------------------+
|225.0.90.90         |46m       |3m                                                               |
+--------------------+----------+-----------------------------------------------------------------+
|Flags     |IGMP Ver |Query Interval |Query Response Interval  |protocol |Advertise Address|
+----------+---------+---------------+-------------------------+---------+-----------------+
|Querier   |2        |125            |10                       |PIM      |12.12.12.11      |
+-------------------------------------------------------------------------------------------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Monitoring VPN Tunnels

Because VPN tunnels synchronize between all Security Group Members, use traditional tools to monitor tunnels.

SmartConsole

You must **not** activate the **Monitoring** Software Blade in the Security Gateway (Security Group) object.

You can still see VPN tunnel status and details information in SmartConsole.

SNMP

- You can use the OID sub-tree **tunnelTable** (.1.3.6.1.4.1.2620.500.9002) in the Check Point MIB to see the VPN status.
- For VSX environments, search for the *SNMP Monitoring* section in the *R80.20SP Quantum Maestro VSX Administration Guide* for VSX-related SNMP information.

CLI Tools

Note - In a VSX environment, you must run these commands from the context of the applicable Virtual System.

Use these commands:

- To see VPN statistics for each Security Group Member, run in the Expert mode:

  ```
  cpstat -f all vpn
  ```

- To monitor VPN tunnels for each Security Group Member, run in the Expert mode:

  ```
  vpn tu
  ```

  VPN tunnels are synchronized to all Security Group Members. Therefore, you can run this command from the scope of one Security Group Member.

- To monitor VPN tunnels in the non-interactive mode, run in Gaia gClish:

  ```
  vpn shell tunnels
  ```

Traceroute (asg_tracert)

Description

Use the "`asg_tracert`" command in Gaia gClish or the Expert mode to show correct `tracert` results on the Security Group.

The native "`tracert`" cannot handle the "`tracert`" pings correctly because of the stickiness mechanism used in the Security Group Firewall.

The "`asg_tracert`" command supports all native options and parameters of the `tracert` command.

Syntax

```
asg_tracert <IP Address> [<tracert Options>]
```

Parameters

Parameter	Description
<IP Address>	Specifies the destination IP address.
<tracert Options>	Specifies the native `tracert` command options.

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_tracert 100.100.100.99
  traceroute to 100.100.100.99 (100.100.100.99), 30 hops max, 40 byte packets
   1   (20.20.20.20)  0.722 ms  0.286 ms  0.231 ms
   2   (100.100.100.99)  1.441 ms  0.428 ms  0.395 ms
[Expert@MyChassis-ch0x-0x:0]#
```

Multi-blade Traffic Capture (tcpdump -mcap, tcpdump -view)

Description

Use the "`tcpdump`" commands in Gaia gClish to capture and show traffic that is sent and received by Security Group Members in the Security Group.

These commands are enhancements to the standard `tcpdump` utility:

Command	Description
`tcpdump -mcap`	Saves packets from specified Security Group Members to a capture file.
`tcpdump -view`	Shows packets from the specified capture file, including the Security Group Member ID.

Note - Use the "`g_tcpdump`" command in the Expert mode.

Syntax

```
tcpdump [-b <SGM IDs>] -mcap -w <Output File> [<tcpdump Options>]
tcpdump -view -r <Input File> [<tcpdump Options>]
```

Note - To stop the capture and save the data to the capture file, press **CTRL+C** at the prompt.

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)

Parameter	Description

`-w <Output File>`	Saves the captured packets at the specified path in a file with the specified the name.
	This output file contains captured packets from all specified Security Group Members.
	In the same directory, the command saves additional output files for each Security Group Member.
	The names of these additional files are: `<SGM ID>_<Specified Name of Output File>`
	Example:
	■ The specified full path is: `/tmp/capture.cap`
	■ The additional capture files are:
	`/tmp/1_1_capture.cap`
	`/tmp/1_2_capture.cap`
	`/tmp/1_3_capture.cap`
	and so on

`-r <Input File>`	Reads the captured packets (in the `tcpdump` format) from the specified path from a file with the specified the name.
`<tcpdump Options>`	Standard `tcpdump` parameters. See the `tcpdump` manual page - https://linux.die.net/man/8/tcpdump.

Examples

Example 1 - Capture packets on all Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > tcpdump -mcap -w /tmp/capture.cap
Capturing packets...
Write "stop" and press enter to stop the packets capture process.
1_01:
tcpdump: listening on eth1-Mgmt4, link-type EN10MB (Ethernet), capture size 96 bytes

Clarification about this output:
At this moment, an administrator pressed the CTRL+C keys

stop
Received user request to stop the packets capture process.

Copying captured packets from all SGMs...
Merging captured packets from SGMs to /tmp/capture.cap...
Done.
[Global] MyChassis-ch01-01>
```

Example 2 - Capture packets from specified Security Group Members and interfaces

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > tcpdump -b 1_1,1_3,2_1 -mcap -w /tmp/capture.cap -nnni eth1-Mgmt4
... ...
[Global] MyChassis-ch01-01 >
```

Example 3 - Show captured packets from a file

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> tcpdump -view -r /tmp/capture.cap
Reading from file /tmp/capture.cap, link-type EN10MB (Ethernet)
 [1_3] 14:11:57.971587 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 45
 [2_3] 14:12:07.625171 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 45
 [2_3] 14:12:09.974195 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 37
 [2_1] 14:12:09.989745 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 45
 [2_3] 14:12:10.022995 IP 0.0.0.0.cp-cluster > 172.23.9.0.cp-cluster: UDP, length 32
... ...
[Global] MyChassis-ch01-01>
```

Monitoring Management Interfaces Link State

By default, Security Group monitors the link state only on data ports `(eth<X>-<YZ>)`.

The Management Monitor feature uses SNMP to monitor management ports on the Quantum Maestro Orchestrators.

The link state is sent to all Security Group Members.

The Management Monitor feature is disabled by default.

To enable this feature, run the "`set chassis high-availability mgmt-monitoring on`" command in Gaia gClish of the Security Group.

When the Management Monitor feature is enabled:

- The monitored management ports are included in the Security Group grade mechanism, according to the predefined factors (default is 11).
- The output of the "`asg stat -v`" command shows the Management ports.

  See the "`Chassis Parameters > Ports > Mgmt`" line in the output example below.
- The "`show interfaces`" command in Gaia gClish shows the link state of management interfaces based on this feature mechanism.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> show chassis high-availability mgmt-monitoring
off
[Global] MyChassis-ch01-01> set chassis high-availability mgmt-monitoring on
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> show chassis high-availability mgmt-monitoring
on
[Global] MyChassis-ch01-01> asg stat -v
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 13:10:04 hours                                |
| SGMs                        | 2 / 2                                         |
| Version                     | R80.20SP (Build Number XXX)                   |
-------------------------------------------------------------------------------
| SGM ID                              Chassis 1                               |
|                                     ACTIVE                                  |
-------------------------------------------------------------------------------
|  1                                    ACTIVE                                |
|  2                                    ACTIVE                                |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit        |                       Chassis 1                       | Weight |
-------------------------------------------------------------------------------
| SGMs        |                         2 / 2                         |   6    |
| Ports       |                                                       |        |
|   Standard  |                         8 / 8                         |  11    |
|   Bond      |                         0 / 0                         |  11    |
|   Mgmt      |                         1 / 1                         |  11    |
|   Other     |                         0 / 0                         |   6    |
| Sensors     |                                                       |        |
|   SSMs      |                         2 / 2                         |  11    |
|             |                                                       |        |
| Grade       |                        73 / 73                        |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> show interfaces
+-------------------------------------------------------------------------------------------------------
--------------+
|Interfaces Data
             |
+-------------------------------------------------------------------------------------------------------
--------------+
|Interface      |IPv4 Address                          |Info        |Link State
|Speed|MTU  |Duplex|
|               |MAC  Address                          |            |(ch1)               |
|     |      |
+---------------+--------------------------------------+------------+--------------------+----
-+-----+------+
|eth1-Mgmt1     |172.23.19.53/24                       |Ethernet    |(Up)                |10G
|1500 |Full  |
|               |00:1c:7f:62:91:94                     |            |                    |
|     |      |
+---------------+--------------------------------------+------------+--------------------+----
-+-----+------+
|Sync           |192.0.2.1/24                          |Ethernet    |(up)                |10G
|1500 |Full  |
|               |00:1c:7f:01:04:fe                     |            |                    |
|     |      |
+---------------+--------------------------------------+------------+--------------------+----
-+-----+------+
... ... output was truncated for brevity ... ...
```

Performance Monitoring and Control

This section provides commands to monitor and control the performance of Security Group Members.

Monitoring Performance (asg perf)

Description

Use the "`asg perf`" command in Gaia gClish or the Expert mode to monitor continuously the key performance indicators and load statistics.

There are different commands for IPv4 and IPv6 traffic.

You can show the performance statistics for IPv4 traffic, IPv6 traffic, or for all traffic.

The command output automatically updates after a predefined interval (default is 10 seconds).

To stop the command and return to the command line, press the **e** key.

Syntax

```
asg perf -h
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-k] [-v] [-vv] [-p] [{-4 | -6}] [-c]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-k] [-e] [--delay <Seconds>]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-v] [-vv [mem [{fwk | cpd | fwd | all_daemons}]]]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-v] [-vv [cpu [{1m | 1h | 24h}]]]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.
`-v`	Shows statistics for each Security Group Member. Adds a performance summary for each Security Group Member.
`-vv`	Shows statistics for each Virtual System. **Note** - This parameter is only relevant in a VSX environment.

Parameter	Description
`mem [{fwk | cpd | fwd | all_daemons}]`	Shows memory usage for each daemon. Use this with the "`-vv`" parameter. Valid values: ■ `fwk` (default) ■ `fwd` ■ `cpd` ■ `all_daemons`
`cpu [{1m | 1h | 24h}]`	Shows CPU usage for a specified period of time. Use this with the "`-vv`" parameter. Valid values: ■ `1m` - The last 60 seconds (default) ■ `1h` - The last hour ■ `24h` - The last 24 hours
`-p`	Shows detailed statistics and traffic distribution between these paths on the Active Site: ■ Acceleration path (SecureXL) ■ Medium path (PXL) ■ Slow path (Firewall)
`{-4 | -6}`	■ `-4` - Shows IPv4 information only. ■ `-6` - Shows IPv6 information only. If no value is specified, the combined performance information shows for both IPv4 and IPv6.
`-c`	Shows percentages instead of absolute values.
`-k`	Shows peak (maximum) system performance values.
`-e`	Resets the peak values and deletes all peaks files and system history files.
`--delay <`*`Seconds`*`>`	Temporarily changes the update interval for the current "`asg perf`" session. Enter a delay value in seconds. The default delay is 10 seconds.

Notes:

- The "`-b <SGM IDs>`" and "`-vs <VS IDs>`" parameters must be at the beginning of the command syntax.
  If both parameters are used, "`-b <SGM IDs>`" must be first.
- If your Security Group is **not** configured in VSX mode, the VSX-related commands are not available.
  They do not appear when you run the "`asg perf -h`" command.

Examples

Example 1 - Summary without Parameters (asg perf)

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf
Thu May 21 08:17:24 IDT 2015
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: 0
+-----------------------------------------------------------------+
|Performance Summary                                              |
+-------------------------------------------+---------------+
|Name                                       |Value          |
+-------------------------------------------+---------------+
|Throughput                                 |751.6 K        |
|Packet rate                                |733            |
|Connection rate                            |3              |
|Concurrent connections                     |142            |
|Load average                               |2%             |
|Acceleration load (avg/min/max)            |1%/0%/4%       |
|Instances load (avg/min/max)               |2%/0%/8%       |
|Memory usage                               |10%            |
+-------------------------------------------+---------------+
 * Instances / Acceleration Cores: 8 / 4
 * Activated SWB: FW,IPS
[Global] MyChassis-ch01-01>
```

Notes:

- By default, absolute values are shown.
- Unless otherwise specified, the combined statistics for IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the Active Security Group Member only.

Example 2 - Performance Summary (asg perf -v)

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf -vs all -v -vv cpu 24h
Tue Oct 22 07:23:37 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-------------------------------------------------------------------------------+
|Performance Summary                                                            |
+-----------------------------------------+-------------+-------------+
|Name                                     |Value        |IPv4%        |
+-----------------------------------------+-------------+-------------+
|Throughput                               |10.2 K       |100%         |
|Packet rate                              |11           |100%         |
|Connection rate                          |0            |N/A          |
|Concurrent connections                   |22           |100%         |
|Load average                             |7%           |             |
|Acceleration load (avg/min/max)          |6%/6%/6%     |             |
|Instances load (avg/min/max)             |5%/4%/9%     |             |
|Memory usage                             |55%          |             |
+-----------------------------------------+-------------+-------------+

+-------------------------------------------------------------------------------+
|Per SGM Distribution Summary                                                   |
+-----+-----------+--------+--------+--------+----------+----------+------+
|SGM  |Throughput |Packet  |Conn.   |Concu.  |Accel.    |Instances |Mem.  |
|ID   |           |Rate    |Rate    |Conn    |Cores%    |Cores%    |Usage%|
+-----+-----------+--------+--------+--------+----------+----------+------+
|1_01 |10.2 K     |11      |0       |22      |6/6/6     |5/4/9     |55%   |
+-----+-----------+--------+--------+--------+----------+----------+------+
|Total|10.2 K     |11      |0       |22      |6/6/6     |5/4/9     |55%   |
+-----+-----------+--------+--------+--------+----------+----------+------+

+-----------------------------------+
|Per VS CPU Usage Summary           |
+-----+---------+---------+---------+
|VS ID|Avg. Cpu%|Min. Cpu%|Max. Cpu%|
|     |         |(SGM id) |(SGM id) |
+-----+---------+---------+---------+
| 0   |2        |1  (1_02)|2  (1_01)|
| 1   |0        |0  (1_01)|0  (1_04)|
+-----+---------+---------+---------+
* CPU stats is aggregated over the last 24hrs
[Global] MyChassis-ch01-01>
```

Make sure to enable the resource control monitoring on all Security Group Members.

Run in the Expert mode on the Security Group:

```
g_fw vsx resctrl monitor enable
```

By default, absolute values are shown.

Notes:

- Average, minimum and maximum values are calculated across all active Security Group Members.
- The Security Group Member ID with the minimum and maximum value shows in brackets for each Security Group Member.

- Unless otherwise specified, the combined statistics for both IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the active Security Group Member only.

Example 3 - Detailed Statistics and Traffic Distribution (asg perf -p)

This example the output for the Virtual Systems 0 and 1.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf -vs 0-1 -p
Aggregated statistics (IPv4 and IPv6) of SGMs: all Virtual Systems: 0-1
+-------------------------------------------------------------------------+
|Performance Summary                                                      |
+-----------------------------------------+---------------+-------------+
|Name                                     |Value          |IPv4%        |
+-----------------------------------------+---------------+-------------+
|Throughput                               |1.7 K          |100%         |
|Packet rate                              |2              |100%         |
|Connection rate                          |0              |N/A          |
|Concurrent connections                   |20             |100%         |
|Load average                             |6%             |             |
|Acceleration load (avg/min/max)          |5%/5%/5%       |             |
|Instances load (avg/min/max)             |5%/3%/10%      |             |
|Memory usage                             |57%            |             |
+-----------------------------------------+---------------+-------------+
=+-----------------------------------------------------------------------+
|Per Path Distribution Summary                                            |
+------------------+------------+--------------+--------------+-----------+
|                  |Acceleration|Medium        |Firewall      |Dropped    |
+------------------+------------+--------------+--------------+-----------+
|Throughput        |0           |0             |1.7 K         |0          |
|Packet rate       |0           |0             |2             |0          |
|Connection rate   |0           |0             |0             |           |
|Concurrent conn.  |10          |0             |10            |           |
+------------------+------------+--------------+--------------+-----------+
[Global] MyChassis-ch01-01>
```

Example 4 - Per Path Statistics (asg perf -p -v)

This example shows detailed performance information for each Security Group Member and traffic distribution between different paths. It also shows VPN throughput and connections.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf -p -v
Tue Oct 22 07:31:31 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-------------------------------------------------------------+
|Performance Summary                                          |
+-------------------------------------+-----------------------+
|Name                                 |Value                  |
+-------------------------------------+-----------------------+
|Throughput                           |3.3 G                  |
|Packet rate                          |6.2 M                  |
|Connection rate                      |0                      |
|Concurrent connections               |3.4 K                  |
|Load average                         |54%                    |
|Acceleration load (avg/min/max)      |58%/48%/68%            |
|Instances load (avg/min/max)         |3%/1%/5%               |
|Memory usage                         |18%                    |
+-------------------------------------+-----------------------+

+-------------------------------------------------------------------------------------------+
|Per SGM Distribution Summary                                                               |
+-------+------------+------------+-----+-----------+-------------+--------------+------+
|SGM ID |Throughput  |Packet rate |Conn.|Concurrent |Core usage   |Core Instances|Memory|
|       |            |            |Rate |Connections|avg/min/max %|avg/min/max % |Usage |
+-------+------------+------------+-----+-----------+-------------+--------------+------+
|1_01   |644.3 M     |1.2 M       |0    |520        |52/44/62     |6/3/10        |18%   |
|1_02   |526.7 M     |997.1 K     |0    |512        |61/51/68     |2/0/5         |18%   |
|1_03   |526.6 M     |997.0 K     |0    |512        |62/53/73     |2/1/3         |18%   |
|1_04   |526.7 M     |997.0 K     |0    |804        |54/48/60     |2/1/3         |18%   |
|1_05   |526.7 M     |997.1 K     |0    |512        |59/45/76     |3/1/5         |18%   |
|1_06   |526.7 M     |997.1 K     |0    |512        |61/52/70     |4/4/5         |18%   |
+-------+------------+------------+-----+-----------+-------------+--------------+------+
|Total  |3.3 G       |6.2 M       |0    |3.4 K      |58/48/68     |3/1/5         |18%   |
+-------+------------+------------+-----+-----------+-------------+--------------+------+

+-------------------------------------------------------------------------------+
|Per Path Distribution Summary                                                  |
+-------------------------+------------+------------+------------+-------------+
|                         |Acceleration|Medium      |Firewall    |Dropped      |
+-------------------------+------------+------------+------------+-------------+
|Throughput               |3.2 G       |0           |2.1 M       |117.6 M      |
|Packet rate              |6.0 M       |0           |1.4 K       |222.8 K      |
|Connection rate          |0           |0           |0           |             |
|Concurrent connections   |3.2 K       |0           |156         |             |
+-------------------------+------------+------------+------------+-------------+

+-------------------------------------+---------------------+
|VPN Performance                      |                     |
+-------------------------------------+---------------------+
|VPN throughput                       |2.9 G                |
|VPN connections                      |3.1 K                |
+-------------------------------------+---------------------+
[Global] MyChassis-ch01-01>
```

Example 5 - Virtual System Memory Summary with Performance Summary (asg perf -vs all -vv mem)

The "`-vv mem`" parameter shows memory usage for each Virtual System across all active Security Group Members.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf -vs all -vv mem
Tue Jul 29 16:05:44 IDT 2014
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: all
+-------------------------------------------------------------+
|Performance Summary                                          |
+---------------------------------------------+---------------+
|Name                                         |Value          |
+---------------------------------------------+---------------+
|Throughput                                   |684.5 K        |
|Packet rate                                  |700            |
|Connection rate                              |3              |
|Concurrent connections                       |144            |
|Load average                                 |2%             |
|Acceleration load (avg/min/max)              |0%/0%/1%       |
|Instances load (avg/min/max)                 |2%/0%/12%      |
|Memory usage                                 |10%            |
+---------------------------------------------+---------------+
 * Instances / Acceleration Cores: 8 / 4
+-------------------------------------------------------------------------------+
|Per VS Memory Summary                                                          |
+--------+-------------+-------------+-------------+-------------+---------+
| VS ID  | User Space  | Memory in   | FWK memory  | Total memory| CPU     |
|        | memory      | Kernel      |             |             | Usage % |
+--------+-------------+-------------+-------------+-------------+---------+
|   0 max|222.3M (1_01)|1.658G (1_04)|47.11M (1_04)|1.880G (1_04)|   N/A   |
|     min|215.8M (1_03)|1.213G (1_01)|45.55M (1_03)|1.249G (1_01)|   N/A   |
+--------+-------------+-------------+-------------+-------------+---------+
|   1 max|56.34M (1_02)|   0K (1_04) |31.16M (1_02)|56.34M (1_02)|   N/A   |
|     min|54.24M (1_01)|   0K (1_04) |29.52M (1_03)|54.24M (1_01)|   N/A   |
+--------+-------------+-------------+-------------+-------------+---------+
* Maximum and minimum values are calculated across all active SGMs
[Global] MyChassis-ch01-01>
```

Notes:

- The Security Group Member that uses the most user space memory on Virtual System 1 is Security Group Member`1_01`
- The Security Group Member that uses the least `fwk` daemon memory on Virtual System 3 is Security Group Member`1_02`
- This information shows only if `vsxmstat` is enabled for `perfanalyze` use
- Make sure that the `vsxmstat` feature is enabled (`vsxmstat status_raw`)

Description

Use the "`asg perf`" command in Gaia gClish or the Expert mode to monitor continuously the key performance indicators and load statistics.

There are different commands for IPv4 and IPv6 traffic.

You can show the performance statistics for IPv4 traffic, IPv6 traffic, or for all traffic.

The command output automatically updates after a predefined interval (default is 10 seconds).

To stop the command and return to the command line, press the **e** key.

Syntax

```
asg perf -h
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-k] [-v] [-vv] [-p] [{-4 | -6}] [-c]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-k] [-e] [--delay <Seconds>]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-v] [-vv [mem [{fwk | cpd | fwd | all_daemons}]]]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-v] [-vv [cpu [{1m | 1h | 24h}]]]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.
`-v`	Shows statistics for each Security Group Member. Adds a performance summary for each Security Group Member.
`-vv`	Shows statistics for each Virtual System. **Note** - This parameter is only relevant in a VSX environment.

Parameter	Description
`mem [{fwk | cpd | fwd | all_daemons}]`	Shows memory usage for each daemon. Use this with the "`-vv`" parameter. Valid values: ■ `fwk` (default) ■ `fwd` ■ `cpd` ■ `all_daemons`
`cpu [{1m | 1h | 24h}]`	Shows CPU usage for a specified period of time. Use this with the "`-vv`" parameter. Valid values: ■ `1m` - The last 60 seconds (default) ■ `1h` - The last hour ■ `24h` - The last 24 hours
`-p`	Shows detailed statistics and traffic distribution between these paths on the Active Site: ■ Acceleration path (SecureXL) ■ Medium path (PXL) ■ Slow path (Firewall)
`{-4 | -6}`	■ `-4` - Shows IPv4 information only. ■ `-6` - Shows IPv6 information only. If no value is specified, the combined performance information shows for both IPv4 and IPv6.
`-c`	Shows percentages instead of absolute values.
`-k`	Shows peak (maximum) system performance values.
`-e`	Resets the peak values and deletes all peaks files and system history files.
`--delay <`*`Seconds`*`>`	Temporarily changes the update interval for the current "`asg perf`" session. Enter a delay value in seconds. The default delay is 10 seconds.

Notes:

- The "`-b <SGM IDs>`" and "`-vs <VS IDs>`" parameters must be at the beginning of the command syntax.
  If both parameters are used, "`-b <SGM IDs>`" must be first.
- If your Security Group is **not** configured in VSX mode, the VSX-related commands are not available.
  They do not appear when you run the "`asg perf -h`" command.

Examples

Example 1 - Summary without Parameters (asg perf)

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf
Thu May 21 08:17:24 IDT 2015
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: 0
+-----------------------------------------------------------------+
|Performance Summary                                              |
+-------------------------------------------+---------------+
|Name                                       |Value          |
+-------------------------------------------+---------------+
|Throughput                                 |751.6 K        |
|Packet rate                                |733            |
|Connection rate                            |3              |
|Concurrent connections                     |142            |
|Load average                               |2%             |
|Acceleration load (avg/min/max)            |1%/0%/4%       |
|Instances load (avg/min/max)               |2%/0%/8%       |
|Memory usage                               |10%            |
+-------------------------------------------+---------------+
 * Instances / Acceleration Cores: 8 / 4
 * Activated SWB: FW,IPS
[Global] MyChassis-ch01-01>
```

Notes:

- By default, absolute values are shown.
- Unless otherwise specified, the combined statistics for IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the Active Security Group Member only.

Example 2 - Performance Summary (asg perf -v)

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf -vs all -v -vv cpu 24h
Tue Oct 22 07:23:37 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-------------------------------------------------------------------------------+
|Performance Summary                                                            |
+-----------------------------------------+-------------+-------------+
|Name                                     |Value        |IPv4%        |
+-----------------------------------------+-------------+-------------+
|Throughput                               |10.2 K       |100%         |
|Packet rate                              |11           |100%         |
|Connection rate                          |0            |N/A          |
|Concurrent connections                   |22           |100%         |
|Load average                             |7%           |             |
|Acceleration load (avg/min/max)          |6%/6%/6%     |             |
|Instances load (avg/min/max)             |5%/4%/9%     |             |
|Memory usage                             |55%          |             |
+-----------------------------------------+-------------+-------------+

+-------------------------------------------------------------------------------+
|Per SGM Distribution Summary                                                   |
+-----+-----------+--------+--------+--------+----------+----------+------+
|SGM  |Throughput |Packet  |Conn.   |Concu.  |Accel.    |Instances |Mem.  |
|ID   |           |Rate    |Rate    |Conn    |Cores%    |Cores%    |Usage%|
+-----+-----------+--------+--------+--------+----------+----------+------+
|1_01 |10.2 K     |11      |0       |22      |6/6/6     |5/4/9     |55%   |
+-----+-----------+--------+--------+--------+----------+----------+------+
|Total|10.2 K     |11      |0       |22      |6/6/6     |5/4/9     |55%   |
+-----+-----------+--------+--------+--------+----------+----------+------+

+-----------------------------------+
|Per VS CPU Usage Summary           |
+-----+---------+---------+---------+
|VS ID|Avg. Cpu%|Min. Cpu%|Max. Cpu%|
|     |         |(SGM id) |(SGM id) |
+-----+---------+---------+---------+
| 0   |2        |1  (1_02)|2  (1_01)|
| 1   |0        |0  (1_01)|0  (1_04)|
+-----+---------+---------+---------+
* CPU stats is aggregated over the last 24hrs
[Global] MyChassis-ch01-01>
```

Make sure to enable the resource control monitoring on all Security Group Members.

Run in the Expert mode on the Security Group:

```
g_fw vsx resctrl monitor enable
```

By default, absolute values are shown.

Notes:

- Average, minimum and maximum values are calculated across all active Security Group Members.
- The Security Group Member ID with the minimum and maximum value shows in brackets for each Security Group Member.

- Unless otherwise specified, the combined statistics for both IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the active Security Group Member only.

Example 3 - Peak Values (asg perf -p)

This example shows peak values for one Virtual System.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf -vs 0-1 -p
Aggregated statistics (IPv4 and IPv6) of SGMs: all Virtual Systems: 0-1
+-------------------------------------------------------------------------+
|Performance Summary                                                      |
+-----------------------------------------+---------------+-------------+
|Name                                     |Value          |IPv4%        |
+-----------------------------------------+---------------+-------------+
|Throughput                               |1.7 K          |100%         |
|Packet rate                              |2              |100%         |
|Connection rate                          |0              |N/A          |
|Concurrent connections                   |20             |100%         |
|Load average                             |6%             |             |
|Acceleration load (avg/min/max)          |5%/5%/5%       |             |
|Instances load (avg/min/max)             |5%/3%/10%      |             |
|Memory usage                             |57%            |             |
+-----------------------------------------+---------------+-------------+
=+-----------------------------------------------------------------------+
|Per Path Distribution Summary                                            |
+------------------+------------+--------------+--------------+-----------+
|                  |Acceleration|Medium        |Firewall      |Dropped    |
+------------------+------------+--------------+--------------+-----------+
|Throughput        |0           |0             |1.7 K         |0          |
|Packet rate       |0           |0             |2             |0          |
|Connection rate   |0           |0             |0             |           |
|Concurrent conn.  |10          |0             |10            |           |
+------------------+------------+--------------+--------------+-----------+
[Global] MyChassis-ch01-01>
```

Example 4 - Per Path Statistics (asg perf -p -v)

This example shows detailed performance information for each Security Group Member and traffic distribution between different paths. It also shows VPN throughput and connections.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf -p -v
Tue Oct 22 07:31:31 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-------------------------------------------------------------+
|Performance Summary                                          |
+-------------------------------------+-----------------------+
|Name                                 |Value                  |
+-------------------------------------+-----------------------+
|Throughput                           |3.3 G                  |
|Packet rate                          |6.2 M                  |
|Connection rate                      |0                      |
|Concurrent connections               |3.4 K                  |
|Load average                         |54%                    |
|Acceleration load (avg/min/max)      |58%/48%/68%            |
|Instances load (avg/min/max)         |3%/1%/5%               |
|Memory usage                         |18%                    |
+-------------------------------------+-----------------------+

+-------------------------------------------------------------------------------------------+
|Per SGM Distribution Summary                                                               |
+-------+------------+------------+-----+-----------+-------------+--------------+------+
|SGM ID |Throughput  |Packet rate |Conn.|Concurrent |Core usage   |Core Instances|Memory|
|       |            |            |Rate |Connections|avg/min/max %|avg/min/max % |Usage |
+-------+------------+------------+-----+-----------+-------------+--------------+------+
|1_01   |644.3 M     |1.2 M       |0    |520        |52/44/62     |6/3/10        |18%   |
|1_02   |526.7 M     |997.1 K     |0    |512        |61/51/68     |2/0/5         |18%   |
|1_03   |526.6 M     |997.0 K     |0    |512        |62/53/73     |2/1/3         |18%   |
|1_04   |526.7 M     |997.0 K     |0    |804        |54/48/60     |2/1/3         |18%   |
|1_05   |526.7 M     |997.1 K     |0    |512        |59/45/76     |3/1/5         |18%   |
|1_06   |526.7 M     |997.1 K     |0    |512        |61/52/70     |4/4/5         |18%   |
+-------+------------+------------+-----+-----------+-------------+--------------+------+
|Total  |3.3 G       |6.2 M       |0    |3.4 K      |58/48/68     |3/1/5         |18%   |
+-------+------------+------------+-----+-----------+-------------+--------------+------+

+-------------------------------------------------------------------------------+
|Per Path Distribution Summary                                                  |
+-------------------------+------------+------------+------------+-------------+
|                         |Acceleration|Medium      |Firewall    |Dropped      |
+-------------------------+------------+------------+------------+-------------+
|Throughput               |3.2 G       |0           |2.1 M       |117.6 M      |
|Packet rate              |6.0 M       |0           |1.4 K       |222.8 K      |
|Connection rate          |0           |0           |0           |             |
|Concurrent connections   |3.2 K       |0           |156         |             |
+-------------------------+------------+------------+------------+-------------+

+-------------------------------------+---------------------+
|VPN Performance                      |                     |
+-------------------------------------+---------------------+
|VPN throughput                       |2.9 G                |
|VPN connections                      |3.1 K                |
+-------------------------------------+---------------------+
[Global] MyChassis-ch01-01>
```

Example 5 - Virtual System Memory Summary with Performance Summary (asg perf -vs all -vv mem)

The "`-vv mem`" parameter shows memory usage for each Virtual System across all active Security Group Members.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg perf -vs all -vv mem
Tue Jul 29 16:05:44 IDT 2014
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: all
+-------------------------------------------------------------+
|Performance Summary                                          |
+---------------------------------------------+---------------+
|Name                                         |Value          |
+---------------------------------------------+---------------+
|Throughput                                   |684.5 K        |
|Packet rate                                  |700            |
|Connection rate                              |3              |
|Concurrent connections                       |144            |
|Load average                                 |2%             |
|Acceleration load (avg/min/max)              |0%/0%/1%       |
|Instances load (avg/min/max)                 |2%/0%/12%      |
|Memory usage                                 |10%            |
+---------------------------------------------+---------------+
 * Instances / Acceleration Cores: 8 / 4
+-------------------------------------------------------------------------------+
|Per VS Memory Summary                                                          |
+--------+-------------+-------------+-------------+-------------+---------+
| VS ID  | User Space  | Memory in   | FWK memory  | Total memory| CPU     |
|        | memory      | Kernel      |             |             | Usage % |
+--------+-------------+-------------+-------------+-------------+---------+
|   0 max|222.3M (1_01)|1.658G (1_04)|47.11M (1_04)|1.880G (1_04)|   N/A   |
|     min|215.8M (1_03)|1.213G (1_01)|45.55M (1_03)|1.249G (1_01)|   N/A   |
+--------+-------------+-------------+-------------+-------------+---------+
|   1 max|56.34M (1_02)|   0K (1_04) |31.16M (1_02)|56.34M (1_02)|   N/A   |
|     min|54.24M (1_01)|   0K (1_04) |29.52M (1_03)|54.24M (1_01)|   N/A   |
+--------+-------------+-------------+-------------+-------------+---------+
* Maximum and minimum values are calculated across all active SGMs
[Global] MyChassis-ch01-01>
```

Notes:

- The Security Group Member that uses the most user space memory on Virtual System 1 is Security Group Member `1_01`
- The Security Group Member that uses the least `fwk` daemon memory on Virtual System 3 is Security Group Member `1_02`
- This information shows only if `vsxmstat` is enabled for `perfanalyze` use
- Make sure that the `vsxmstat` feature is enabled (`vsxmstat status_raw`)

Performance Hogs (asg_perf_hogs)

In This Section:

You can run tests to check for software components that decrease (hog) performance.

Syntax

Description

You can run:

- The "`asg_perf_hogs`" command in the Expert mode
- The "`show smo verifiers report name Performance_hogs`" command in Gaia gClish

Notes:

- When you run the "`asg_perf_hogs`" command by itself, you can get the full details of all the tests it runs.
- When you run the "`show smo verifiers report name Performance_hogs`" command, it shows a general result of "`asg_perf_hogs`" test output.
- If all of the "`asg_perf_hogs`" tests pass, the "`show smo verifiers report name Performance_hogs`" command shows **Passed**.
- If even one of the "`asg_perf_hogs`" tests fails, the "`show smo verifiers report name Performance_hogs`" command shows **Failed (!)**.

Syntax

```
asg_perf_hogs
```

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_perf_hogs
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | PPACK debug flags                                  |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [FAILED] | routed trace options                               |
-----------------------------------------------------------------

Found the following issues:
-----------------------------------------------------------------
[ All] routed trace options are set: Cluster; igmp:All; pim:All
[Expert@MyChassis-ch0x-0x:0]#
```

Configuration

Configure the "`asg_perf_hogs`" behavior in the `$SMODIR/conf/performance_hogs.conf` file.

```
[tests]
long_running_procs=1
accel_off=1
sim_debug_flags=1
fw1_debug_flags=1
local_logging=1
disabled_templates=1
correction_table_entries=1
routing_cache_entries=1
swap_saturation=1
delayed_notifications=1
neighbour_table_overflow=1
soft_lockups=1
standby_chassis_load=1
routed_trace_options=1
peak_connections=1
[correction_table_entries]
threshold=10
[long_running_procs]
elapsed_time=60
processes_to_check=("fw ctl zdebug" "fw ctl debug" "fw ctl kdebug" "fw monitor" "tcpdump")
[routing_cache_entries]
threshold=90
[swap_saturation]
threshold=50
[neighbour_table_overflow]
timeout=3600
[soft_lockups]
timeout=3600
[standby_chassis_load]
threshold=50
[peak_connections]
threshold=90
[disabled_templates]
#max_rule_num=999
```

The [tests] Section

In the **[tests]** section of the `$SMODIR/conf/performance_hogs.conf` file you enable and disable tests to run.

Note - Not all the tests can be configured.

To enable or disable a test:

In the "`[tests]`" section, set the applicable value for the applicable test:

- To enable the test:

  ```
  <Test Name>=1
  ```

- To disable the test:

  ```
  <Test Name>=0
  ```

To configure a test:

Step	Instructions
1	Find the configuration section for the test in the `$SMODIR/conf/performance_hogs.conf` file. If it does not exist, add the section with this format: `[<Test Name>]`
2	Change or add the parameters for the test. See the tables below for allowed parameters.

Below are the descriptions of some of the tests in the "`[tests]`" section in the `$SMODIR/conf/performance_hogs.conf` file.

long_running_procs

The "`long_running_procs`" test confirms that certain processes do not run longer than the configured time.

Note - This test runs in contexts of all Virtual Systems.

Parameters:

Parameter	Description
`elapsed_time`	Longest time in seconds a process should run Default: 60 seconds. Minimum recommended value: 30 seconds.

`processes_to_check`	List of processes to check:
	You must enclose each process in double quotes.
	You must enter a space before another test.
	Default:
	`"fw ctl zdebug" "fw ctl debug" "fw ctl kdebug" "fw monitor" "tcpdump"`
	Example:
	`processes_to_check=("fw ctl zdebug" "fw ctl debug" "fw ctl kdebug" "fw monitor" "tcpdump")`

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [FAILED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------

Found potential CPU hogging processes:
-----------------------------------------------------------------
Blade    PID     ELAPSED     TIME CMD
[1_01]  1484       03:48 00:00:00 tcpdump -nnni eth1-01

Found the following issues:
-----------------------------------------------------------------
[ All] The process 'tcpdump' is running for more than 60 seconds
```

accel_off

The "`accel_off`" test confirms that SecureXL is working.

Notes:

- This test has no configuration options.
- The test runs in the context of the current Virtual System only.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [FAILED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[ All] SecureXL acceleration is disabled!
```

fw1_debug_flags

The "`fw1_debug_flags`" test confirms that Firewall debug flags that are not enabled by default, stay in the disabled position.

Notes:

- This test has no configuration options.
- This test runs in contexts of all Virtual Systems.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [FAILED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[ All] FW1 debug flags are set:; Module: fw; ; Flags: error warning packet
```

local_logging

The "`local_logging`" test confirms that logs are written to a Log Server and not locally.

Notes:

- This test has no configuration options.
- This test runs in the context of the current Virtual System only.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [FAILED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[ All] Local logging is active: No connection with log server!
```

routing_cache_entries

The "`routing_cache_entries`" test confirms that the IPv4 route cache capacity is not above a certain threshold.

Threshold is the percent capacity of the IPv4 route cache that should not be exceeded:

- Default: 90%.
- Recommended range: 75 - 95%.

Note - This test runs in the context of the current Virtual System only.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [FAILED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[ All] Routing cache is 93% full (983731 out of 1048576 entries).
```

swap_saturation

The "`swap_saturation`" test confirms that swap file usage is not above the threshold.

Threshold is the percent use of the swap file allowed.

Recommended range: 75 - 99.

Note - This test runs regardless of the Virtual System context.

Example output

```
-------------------------------------------------------------------
|  Status  |  Test performed                                      |
-------------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                            |
| [PASSED] | Disabled NAT Templates                               |
| [PASSED] | FW1 debug flags                                      |
| [PASSED] | Kernel soft lockups                                  |
| [PASSED] | Local logging                                        |
| [PASSED] | Long running processes                               |
| [PASSED] | Neighbour table overflow                             |
| [PASSED] | Routing cache entries                                |
| [PASSED] | SecureXL status                                      |
| [FAILED] | Swap saturation                                      |
| [PASSED] | routed trace options                                 |
-------------------------------------------------------------------
 Found the following issues:
-------------------------------------------------------------------
[ All] Swap saturation is 90%. Total swap space: 1044216 bytes, used: 950000 bytes.
```

neighbour_table_overflow

The "`neighbour_table_overflow`" test confirms that the ARP cache did not overflow.

Timeout is the number of seconds the specifies for how long to look in the `/var/log/messages` file for ARP cache overloaded messages.

Recommended range: 300 - 86400.

Notes:

- To learn how to adjust the ARP cache, see sk43772.
- This test runs regardless of the Virtual System context.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [FAILED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
Found the following issues:
-----------------------------------------------------------------
[ All] Neighbour table overflow occurred during the last 3600 seconds.
Please see solution SK43772 for information how to configure arp cache size.
```

soft_lockups

The "`soft_lockups`" test confirms there are no kernel soft lockups during the timeout period.

Timeout is the number of seconds to look back in the `/var/log/messages` file for kernel soft lockup messages:

- Default: 3600 seconds.
- Recommended range: 300 - 86400 seconds.

Note - This test runs regardless of the Virtual System context.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [FAILED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[1_01] Soft lockup occurred during the last 3600 seconds.
```

Setting Port Priority

Description

For each Security Group port, you can set a port priority - high or standard.

Use the "`set chassis high-availability port ... priority ...`" command in Gaia gClish on the Security Group.

Syntax

```
set chassis high-availability port <Name of Interface> priority
<Priority>
```

Parameters

Parameter	Description
<Name of Interface>	Specifies the interface name.
<Priority>	Specifies the port grade. Valid values: ■ `1` - Standard priority ■ `2` - Other priority

Use the "`set chassis high-availability port ... priority ...`" command together with the "`set chassis high-availability factors port ...`" command:

- Set the port grade as standard or high.

  For example, to set the standard grade at 50, run:

  ```
  set chassis high-availability factors port standard 50
  ```

- Set the port to high grade or standard grade.

  For example, to assign the standard port grade to `eth1-01`, run:

  ```
  set chassis high-availability port eth1-01 priority 1
  ```

Searching for a Connection (asg search)

In This Section:

This section describes how to search for a connection in the Connections Table.

Description

Use the "`asg search`" command in Gaia gClish or the Expert mode to:

- Search for a connection or a filtered list of connections.
- See which Security Group Member handles the connection, actively or as backup, and on which Site.

You can run this command directly or in Interactive Mode. In the Interactive Mode, you can enter the parameters in the correct sequence.

The "`asg search`" command also runs a consistency test between Security Group Members.

This command supports both IPv4 and IPv6 connections.

Searching in the Non-Interactive Mode

Syntax

```
asg search -help
```

```
asg search [-v] [-vs <VS IDs>] [<Source IP Address> <Source Port> <Destination IP Address> <Destination Port> <Protocol>]
```

Parameters

Parameter	Description
No Parameters	Runs in the interactive mode.
`-help`	Shows the built-in help.

Parameter	Description
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.
<Source IP Address>	Specifies the source IPv4 or IPv6 address.
<Source Port>	Specifies the source port number. See *IANA Service Name and Port Number Registry*.
<Destination IP Address>	Specifies the destination IPv4 or IPv6 address.
<Destination Port>	Specifies the destination port number. See *IANA Service Name and Port Number Registry*.
<Protocol>	Specifies the IP Protocol name or number. See *IANA Protocol Numbers*.
`-v`	Shows connection indicators for: ■ **A** - Active Security Group Member ■ **B** - Backup Security Group Member ■ **F** - Firewall Connections table ■ **S** - SecureXL Connections table ■ **C** - Correction Layer table This is in addition to the indicators for Active and Backup Security Group Members.

Notes:

- You must enter the all parameters in the sequence as appears in the above syntax.
- You can enter "`\*`" as a wildcard parameter (meaning, any value).
- The "`-vs`" parameter is only available for a Security Group in VSX mode.

Examples

Example 1 - Search for one IPv4 source address, one IPv4 destination address, all ports, and the TCP protocol

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg search -v 192.0.2.4 192.0.2.15 \* tcp
Lookup for conn: <192.0.2.4, 192.0.2.15, *, tcp>, may take few seconds...

<192.0.2.4, 1130,  192.0.2.15, 49829, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36323, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49851, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36308, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36299, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49835, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49856, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36331, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49857, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49841, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36315, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49859, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36300, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36301, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]

Legend:
A - Active SGM
B - Backup SGM
C - Correction Layer table
F - Firewall connection table
S - SecureXL connection table
[Global] MyChassis-ch01-01>
```

Example 2 - Search for one IPv6 source address, all destination IP addresses, destination port 8080, and TCP protocol

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg search 2620:0:2a03:16:2:33:0:1 \* 8080 tcp

<2620:0:2a03:16:2:33:0:1, 52117, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
<2620:0:2a03:16:2:33:0:1, 62775, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
<2620:0:2a03:16:2:33:0:1, 54378, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
Legend:
A - Active SGM
B - Backup SGM
[Global] MyChassis-ch01-01>
```

Example 3 - Search for all sources, destinations, ports, and protocols for VS0

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg search -vs 0 \* \* \* \* \*.
Lookup for conn: <*, *, *, *, *>, may take few seconds...

<172.23.9.130, 18192, 172.23.9.138, 43563, tcp> -> [1_01 A]
<172.23.9.130, 32888, 172.23.9.138, 257, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.47.14, 52120, tcp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 32963, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.47.14, 52104, tcp> -> [1_01 A]
<255.255.255.255, 67, 0.0.0.0, 68, udp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 32864, tcp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 32888, tcp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 33465, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.40.23, 65515, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.47.14, 52493, tcp> -> [1_01 A]
<172.23.9.130, 18192, 172.23.9.138, 49059, tcp> -> [1_01 A]
<172.23.9.130, 18192, 172.23.9.138, 33356, tcp> -> [1_01 A]
<172.23.9.138, 33356, 172.23.9.130, 18192, tcp> -> [1_01 A]
<172.23.9.138, 43563, 172.23.9.130, 18192, tcp> -> [1_01 A]
<172.23.9.130, 32864, 172.23.9.138, 257, tcp> -> [1_01 A]
<0.0.0.0, 68, 255.255.255.255, 67, udp> -> [1_01 A]
<172.23.9.130, 32963, 172.23.9.138, 257, tcp> -> [1_01 A]
<172.23.9.130, 33465, 172.23.9.138, 257, tcp> -> [1_01 A]
<194.29.47.14, 52120, 172.23.9.130, 22, tcp> -> [1_01 A]
<194.29.47.14, 52104, 172.23.9.130, 22, tcp> -> [1_01 A]
<fe80::d840:5de7:8dbe:2345, 546, ff02::1:2, 547, udp> -> [1_01 A]
<194.29.47.14, 52493, 172.23.9.130, 22, tcp> -> [1_01 A]
<172.23.9.138, 49059, 172.23.9.130, 18192, tcp> -> [1_01 A]
<194.29.40.23, 65515, 172.23.9.130, 22, tcp> -> [1_01 A]
Legend:
A - Active SGM
B - Backup SGM
[Global] MyChassis-ch01-01>
```

Searching in the Interactive Mode

In the Interactive Mode, you enter the connection search parameters in the required sequence.

Step	Instructions
1	Connect to the command line on the Security Group.
2	Go to Gaia gClish: enter `gclish` and press Enter.
3	Run the command: `> asg search [-vs <VS IDs>] [-v]`
4	Enter these parameters in the order below: 1. Source IPv4 or IPv6 address. 2. Destination IPv4 or IPv6 address. 3. Destination port number. See *IANA Service Name and Port Number Registry*. 4. IP protocol. See *IANA Protocol Numbers*. 5. Source port number. See *IANA Service Name and Port Number Registry*. **Note** - Press the **Enter** key to enter a wildcard value (meaning, any value).

Example - Search for one IPv4 source and destination

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg search -v

Please enter conn's 5 tuple:
----------------------------
Enter source IP (press enter for wildcard):
 >192.0.2.4
Enter destination IP (press enter for wildcard):
 >192.0.2.15
Enter destination port (press enter for wildcard):
 >
Enter IP protocol ('tcp', 'udp', 'icmp' or enter for wildcard):
 >tcp
Enter source port (press enter for wildcard):
 >
Lookup for conn: <192.0.2.4, *, 192.0.2.15, *, tcp>, may take few seconds...
<192.0.2.4, 37408, 192.0.2.15, 1130, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49670, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49653, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 37406, 192.0.2.15, 1130, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49663, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49658, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 37407, 192.0.2.15, 1130, tcp> -> [2_01 AF, 1_04 AF]

Legend:
A - Active SGM
B - Backup SGM
C - Correction Layer table
F - Firewall connection table
S - SecureXL connection table

[Global] MyChassis-ch01-01>
```

Showing the Number of Firewall and SecureXL Connections (asg_conns)

Description

Use the "`asg_conns`" command in Gaia gClish or the Expert mode to show the number of Firewall and SecureXL connections on each Security Group Member.

Syntax

```
asg_conns -h
asg_conns [-b <SGM IDs>] [-6]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`-6`	Shows only IPv6 connections.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg_conns
1_01:
     #VALS     #PEAK   #SLINKS
       246      1143       246
1_02:
     #VALS     #PEAK   #SLINKS
        45       172        45
1_03:
     #VALS     #PEAK   #SLINKS
        45       212        45
1_04:
     #VALS     #PEAK   #SLINKS
       223       624       223
1_05:
     #VALS     #PEAK   #SLINKS
        45       246        45

Total (fw1 connections table): 604 connections

1_01:
There are 60 conn entries in SecureXL connections table
Total conn entries @ DB 0:  4
Total conn entries @ DB 3:  2
.
.
Total conn entries @ DB 26:  4
Total conn entries @ DB 30:  2
1_02:
There are 16 conn entries in SecureXL connections table
Total conn entries @ DB 0:  2
Total conn entries @ DB 1:  2
.
.
Total conn entries @ DB 26:  2
1_03:
There are 16 conn entries in SecureXL connections table
Total conn entries @ DB 0:  2
Total conn entries @ DB 5:  2
.
.
Total conn entries @ DB 30:  2
1_04:
There are 260 conn entries in SecureXL connections table
Total conn entries @ DB 0:  10
Total conn entries @ DB 1:  6
.
.
Total conn entries @ DB 31:  94
1_05:
There are 16 conn entries in SecureXL connections table
Total conn entries @ DB 2:  2
.
.
Total conn entries @ DB 26:  2

Total (SecureXL connections table): 368 connections
[Global] MyChassis-ch01-01>
```

Packet Drop Monitoring (drop_monitor and asg_drop_monitor)

In This Section:

Important - Starting in Take 209 of R80.20SP Jumbo Hotfix Accumulator (sk155832), the new utility "`drop_monitor`" replaced the previous "`asg_drop_monitor`" utility.

The "drop_monitor" command

Description

Use the "`drop_monitor`" command in the Expert mode to monitor dropped packets on interfaces in real time.

Drop statistics arrive from these modules:

- NICs
- CoreXL
- PSL
- SecureXL

Notes:

- This command opens a monitor session and shows aggregated data from Security Group Members.
  To stop an open session, press **CTRL+C**.
- By default, this utility shows drop statistics for IPv4 traffic.

Syntax

```
drop_monitor -h
```

```
drop_monitor [-d] [-v] [-m <SGM IDs>] [-i <List of Interfaces>]
[-f <Refresh Rate>] [-sf <Query Timeout>] [-le] [-e] [-dm] [-ds]
[-r] [-s] [-v6]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-d` `--debug`	Runs the command in the debug mode.

Parameter	Description
`-v` `--verbose`	Shows detailed drop statistics - for each Security Group Member and all SecureXL statistics.
`-m <SGM IDs>` `--members <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`-i <List of Interfaces>` `--interfaces <List of Interfaces>`	Shows drop statistics for the specified network interfaces. Enter the names of applicable interfaces separated a comma. By default, this utility shows drop statistics only for the backplane interfaces.
`-f <Refresh Rate>` `--refresh-rate <Refresh Rate>`	Specifies the output refresh rate in seconds. The default is 3 seconds.
`-sf <Query Timeout>` `--ssms-refresh-rate <Query Timeout>`	Specifies the query timeout in seconds. The default is 60 seconds.
`-le` `--local-export`	Exports drop statistics from the local Security Group Member in the JSON format.
`-e` `--global-export`	Exports drop statistics from all Security Group Members in the JSON format.
`-dm` `--detailed-members`	Shows drop statistics for each Security Group Member, in addition to the total drop statistics.

Parameter	Description
`-ds` `--detailed-securexl`	Shows detailed drop statistics for SecureXL.
`-r` `--reset`	Resets the statistics counters to 0 before it collects the data. **Note** - Drop statistics are reset for CoreXL, PSL, SecureXL, and backplane interfaces.
`-s` `--include-ssms-stats`	Shows local drop statistics only. Only data links, management links, and downlinks are supported.
`-v6` `--ipv6`	Shows drop statistics for IPv6 traffic.

Example 1 - Default output

```
[Expert@MyChassis-ch0x-0x:0]# drop_monitor

Dropped packets statistics of network interfaces, CoreXL, SecureXL and PSL
+----------+------------------+-------+
| Category | Statistics       | Total |
+----------+------------------+-------+
+----------+------------------+-------+
|          | RX Dropped       |   0   |
|   NIC    | TX Dropped       |   0   |
|          | Qdisc Dropped    |   0   |
+----------+------------------+-------+
|          | Outbound Dropped |   0   |
|  CoreXL  | Inbound Dropped  |   0   |
|          | F2P Dropped      |   0   |
+----------+------------------+-------+
|   PSL    | Total Dropped    |   0   |
|          | Rejected         |   0   |
+----------+------------------+-------+
| SecureXL | Total drops      |   0   |
+----------+------------------+-------+

[Expert@MyChassis-ch0x-0x:0]#
```

Example 2 - Verbose output

```
[Expert@MyChassis-ch0x-0x:0]# drop_monitor -v

Dropped packets statistics of network interfaces, CoreXL, SecureXL and PSL
+----------+----------------------+------+------+-------+
| Category | Statistics           | 1_01 | 1_02 | Total |
+----------+----------------------+------+------+-------+
+----------+----------------------+------+------+-------+
|          | RX Dropped           |  0   |  0   |   0   |
|   NIC    | TX Dropped           |  0   |  0   |   0   |
|          | Qdisc Dropped        |  0   |  0   |   0   |
+----------+----------------------+------+------+-------+
|          | Outbound Dropped     |  0   |  0   |   0   |
|  CoreXL  | Inbound Dropped      |  0   |  0   |   0   |
|          | F2P Dropped          |  0   |  0   |   0   |
+----------+----------------------+------+------+-------+
|   PSL    | Total Dropped        |  0   |  0   |   0   |
|          | Rejected             |  0   |  0   |   0   |
+----------+----------------------+------+------+-------+
|          | XMT error            |  0   |  0   |   0   |
|          | general reason       |  0   |  0   |   0   |
|          | Syn Defender         |  0   |  0   |   0   |
|          | Attack mitigation    |  0   |  0   |   0   |
|          | VPN forwarding       |  0   |  0   |   0   |
|          | corrupted packet     |  0   |  0   |   0   |
|          | hl - spoof viol      |  0   |  0   |   0   |
|          | encrypt failed       |  0   |  0   |   0   |
|          | cluster error        |  0   |  0   |   0   |
|          | anti spoofing        |  0   |  0   |   0   |
|          | monitored spoofed    |  0   |  0   |   0   |
|          | hl - new conn        |  0   |  0   |   0   |
|          | hl - TCP viol        |  0   |  0   |   0   |
|          | F2F not allowed      |  0   |  0   |   0   |
| SecureXL | fragment error       |  0   |  0   |   0   |
|          | Session rate exceed  |  0   |  0   |   0   |
|          | PXL decision         |  0   |  0   |   0   |
|          | template quota       |  0   |  0   |   0   |
|          | drop template        |  0   |  0   |   0   |
|          | sanity error         |  0   |  0   |   0   |
|          | outb - no conn       |  0   |  0   |   0   |
|          | clr pkt on vpn       |  0   |  0   |   0   |
|          | partial conn         |  0   |  0   |   0   |
|          | decrypt failed       |  0   |  0   |   0   |
|          | Connections Limit by |  0   |  0   |   0   |
|          | Source IP exceed its |  0   |  0   |   0   |
|          | local spoofing       |  0   |  0   |   0   |
|          | interface down       |  0   |  0   |   0   |
+----------+----------------------+------+------+-------+

[Expert@MyChassis-ch0x-0x:0]#
```

The "asg_drop_monitor" command

Description

Use the "`asg_drop_monitor`" command in the Expert mode to monitor dropped packets in real time.

Drop statistics arrive from these modules:

- NICs
- Operating System
- CoreXL
- PSL
- SecureXL

Notes:

- This command opens a monitor session and shows aggregated data from Security Group Members.
  To stop an open session, press **CTRL+C**.
- By default, this utility shows drop statistics for IPv4 traffic.

Syntax

```
asg_drop_monitor -h
asg_drop_monitor [-r] [-6]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-r`	Resets statistics counters to 0 before it collects the data.
`-ssm [-t <Timeout>]`	This parameter is not supported on Maestro Security Groups (Known Limitation MBS-5478).
`-6`	Shows drop statistics only for IPv6 traffic.

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_drop_monitor

(IPv4 Drop Statistics - All Blades)
Wed Feb 27 11:04:51 EST 2019
NICs drops (Rx):
18415

IP Stack qdisc drops (Tx):
0

CoreXL queue drops (F2F):
14781348

CoreXL queue drops (PXL F2P)
0

PSL drops(total):
0

PSL rejects:
0

Ppak drops:
Displaying aggregated data from blades: all

Reason                Value              Reason                Value
--------------------  ---------------    --------------------  ---------------
general reason                8881796    CPASXL decision                     0
PSLXL decision                      0    clr pkt on vpn                      0
encrypt failed                      0    drop template                       0
decrypt failed                      0    interface down                      0
cluster error                       0    XMT error                           0
anti spoofing                       0    local spoofing                      0
sanity error                        0    monitored spoofed                   0
QOS decision                        0    C2S violation                       0
S2C violation                       0    Loop prevention                     0
DOS Fragments                       0    DOS IP Options                      0
DOS Blacklists                      0    DOS Penalty Box                     0
DOS Rate Limiting                   0    Syn Attack                          0
Reorder                             0    Expired Fragments                   0
[Expert@MyChassis-ch0x-0x:0]#
```

Hardware Monitoring and Control

You can monitor the hardware components of your system.

Showing Hardware State (asg stat)

Description

Use the "`asg stat`" command in Gaia gClish or the Expert mode to show the state of the system and hardware components.

The command output shows:

- Security Gateway Mode (Gateway or VSX)
- Number of members in the Security Group
- Number of Virtual Systems
- Information related to VSX configuration
- Uptime
- Software Version

Syntax

```
asg stat
      -h
      -i list_all
      -i sgm_info
      -i tasks
      -v [-amw]
      vs [all [-p]]
```

Note - If you run this command in the context of a Virtual System, the output applies only to that Virtual System.

Parameters

Parameter	Description
No Parameters	Shows the Security Group status (short output).
`-h`	Shows the built-in help.

Parameter	Description
`-i list_all`	Shows: ■ The IDs of the Security Group Members, their state and IP addresses ■ Tasks and on which Security Group Member they run
`-i sgm_info`	Shows the IDs of the Security Group Members, their state and IP addresses
`-i tasks`	Shows the list of Tasks and on which Security Group Member they run: ■ **SMO** - Single Management Object ■ **General** - General ■ **LACP** - Interface Bonding ■ **CH Monitor** - Site state monitor ■ **DR Manager** - Dynamic Routing manager ■ **UIPC** - Unique IP Address for each Site ■ **Alert** - Alerts
`-v [-amw]`	Shows the detailed Security Group status (verbose output). The "`-amw`" parameter shows the update status for the applicable Software Blades.
`vs [all [-p]]`	Shows the VSX information: ■ `vs` Shows general output for a Virtual System. Run this command in the context of the applicable Virtual System. ■ `vs all` Output also shows all Virtual Systems. ■ `vs all -p` Output shows a summary health status for all Virtual Systems. For more information on a specific Virtual System, run the "`asg stat vs`" command in the context of the Virtual System.

Examples

Example 1 - Default Output (asg stat)

Syntax

```
asg stat
```

Example output from a Dual Site configuration

```
[Expert@MyChassis-ch0x-0x:0]# asg stat
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Chassis Mode                | Active Up                                     |
| Up time                     | 21:29:56 hours                                |
| SGMs                        | 12/12                                         |
| Version                     | R80.20SP (Build Number XXX)                   |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |          Chassis 1            |          Chassis 2           |
-------------------------------------------------------------------------------
| SGMs         |            6 / 6              |            6 / 6             |
| Ports        |            5 / 5              |            5 / 5             |
| SSMs         |            2 / 2              |            2 / 2             |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example output from a Single Site configuration

```
[Expert@MyChassis-ch0x-0x:0]# asg stat
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 02:10:27 hours                                |
| SGMs                        | 30/30                                         |
| Version                     | R80.20SP (Build Number XXX)                   |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |                          Chassis 1                         |
-------------------------------------------------------------------------------
| SGMs         |                            30 / 30                         |
| Ports        |                             4 / 4                          |
| SSMs         |                             2 / 2                          |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2 - Detailed Output (asg stat -v)

Syntax

```
asg stat -v
```

Example output from a Dual Site configuration - top section

This output shows a Security Group with 12 Security Group Members in the Active (UP) state (out of total 12).

The Site #1 is Active. The Site #2 is Standby.

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -v
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Chassis Mode                | Active Up                                     |
| Up time                     | 21:30:50 hours                                |
| SGMs                        | 12/12                                         |
| Version                     | R80.20SP (Build Number XXX)                   |
-------------------------------------------------------------------------------
| SGM ID             Chassis 1                          Chassis 2             |
|                    ACTIVE                             STANDBY               |
-------------------------------------------------------------------------------
|  1                   ACTIVE                             ACTIVE              |
|  2                   ACTIVE                             ACTIVE              |
|  3                   ACTIVE                             ACTIVE              |
|  4                   ACTIVE                             ACTIVE              |
|  5                   ACTIVE                             ACTIVE              |
|  6                   ACTIVE                             ACTIVE              |
-------------------------------------------------------------------------------
... output was truncated for brevity - the example continues below ...
```

Example output from a Single Site configuration - top section

This output shows a Security Group with 30 Security Group Members in the Active (UP) state (out of total 30).

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -v
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 02:10:39 hours                                |
| SGMs                        | 30/30                                         |
| Version                     | R80.20SP (Build Number XXX)                   |
-------------------------------------------------------------------------------
| SGM ID                            Chassis 1                                 |
|                                   ACTIVE                                    |
-------------------------------------------------------------------------------
|  1                                  ACTIVE                                  |
|  2                                  ACTIVE                                  |
|  3                                  ACTIVE                                  |
... output was truncated for brevity ...
|  30                                 ACTIVE                                  |
-------------------------------------------------------------------------------
... output was truncated for brevity - the example continues below ...
```

Explanation about the output:

Field	Instructions
SGM ID	Identifier of the Security Group Member. The `(local)` is the Security Group Member, on which you ran the command.
State	State of the Security Group Member: ■ `ACTIVE` - The Security Group Member is processing traffic ■ `DOWN` - The Security Group Member is not processing traffic ■ `Detached` - No Security Group Member is detected in a slot **Note** - To change manually the state of the Security Group Member, use the "`g_clusterXL_admin`" command (see *"Configuring the Cluster State (g_clusterXL_admin)" on page 170*).

Example output from a Dual Site configuration - bottom section

```
... output was truncated for brevity - the example starts above ...
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |        Chassis 1          |        Chassis 2          | Weight |
-------------------------------------------------------------------------------
| SGMs         |          6 / 6            |          6 / 6            |   6    |
| Ports        |                           |                           |        |
|   Standard   |          5 / 5            |          5 / 5            |  11    |
|   Bond       |          0 / 0            |          0 / 0            |  11    |
|   Other      |          0 / 0            |          0 / 0            |   6    |
| Sensors      |                           |                           |        |
|   SSMs       |          2 / 2            |          2 / 2            |  11    |
|              |                           |                           |        |
| Grade        |        113 / 113          |        113 / 113          |   -    |
-------------------------------------------------------------------------------
| Minimum grade gap for chassis failover:                                 11  |
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
|     Sync to Standby chassis:   Enabled                                      |
-------------------------------------------------------------------------------
| Chassis HA mode:              Active Up                                     |
-------------------------------------------------------------------------------
```

Example output from a Single Site configuration - bottom section

```
... output was truncated for brevity - the example starts above ...
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |                      Chassis 1                       | Weight |
-------------------------------------------------------------------------------
| SGMs         |                       30 / 30                        |   6    |
| Ports        |                                                      |        |
|   Standard   |                        4 / 4                         |  11    |
|   Bond       |                        0 / 0                         |  11    |
|   Other      |                        0 / 0                         |   6    |
| Sensors      |                                                      |        |
|   SSMs       |                        2 / 2                         |  11    |
|              |                                                      |        |
| Grade        |                      246 / 246                       |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
```

Note - In the notation "*<Number> / <Number>*", the left number shows the number of components that in the UP state, and the right number shows the number the components that must be in the UP state.
For example, on the **SGMs** line, "30 / 30" means that there are currently 30 Security Group Members in the UP state out of the 30 that must be in the UP state.

Field	Description

Grade	The sum of the grades of all components.
	The grade of each component is the unit weight multiplied by the number of components that are in the UP state.
	You can configure the unit weight of each component to show the importance of the component in the system.
	To configure the unit weight, run in Gaia gClish:
	`set chassis high-availability factors <Hardware Component>`
	For example, to change the weight of the Security Group Member to 12, run in Gaia Clish on that Security Group Member:
	`set chassis high-availability factors sgm 12`
	See *"Configuring Security Group High Availability" on page 372*.
	If you run the "`asg stat -v`" command, the output shows a greater unit weight and system grade.

Minimum grade gap for chassis failover	Site failover occurs to the Site with the higher grade only if its grade is greater than the other Site by more than the minimum gap. Minimum threshold for traffic processing - the minimum grade required for the Site to become Active.

Field	Description
Synchronization	Status of synchronization between Security Group Members: ■ Within a Site - between Security Group Members located in the same Security Group ■ Between two Sites - between Security Group Members located in different Sites ■ Exception Rules - exception rules configured by an administrator with the "`g_sync_exception`" command.

Example 3 - List of Tasks (asg stat -i tasks)

Syntax

```
asg stat -i tasks
```

Example output from a Dual Site configuration

The SMO task runs on Site #2 - on the Security Group Member #3, on which you ran this command (see the string "`(local)`").

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |                            |         3(local)           |
| General (1)        |         2                  |         3(local)           |
| LACP (2)           |         2                  |         3(local)           |
| CH Monitor (3)     |         2                  |         3(local)           |
| DR Manager (4)     |                            |         3(local)           |
| UIPC (5)           |         2                  |         3(local)           |
| Alert (6)          |                            |         3(local)           |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
[Expert@MyChassis-ch0x-0x:0]# member 2_4
Moving to member 2_4
... ...
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |                            |         3                  |
| General (1)        |         2                  |         3                  |
| LACP (2)           |         2                  |         3                  |
| CH Monitor (3)     |         2                  |         3                  |
| DR Manager (4)     |                            |         3                  |
| UIPC (5)           |         2                  |         3                  |
| Alert (6)          |                            |         3                  |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example output from all Security Group Members (in our example, there are two on each Site):

```
[Expert@MyChassis-ch0x-0x:0]# g_all asg stat -i tasks
1_01:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1(local)           |                            |
| General (1)        |         1(local)           |         1                  |
| LACP (2)           |         1(local)           |         1                  |
| CH Monitor (3)     |         1(local)           |         1                  |
| DR Manager (4)     |         1(local)           |                            |
| UIPC (5)           |         1(local)           |         1                  |
| Alert (6)          |         1(local)           |                            |
-------------------------------------------------------------------------------

1_02:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1                  |
| LACP (2)           |         1                  |         1                  |
| CH Monitor (3)     |         1                  |         1                  |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1                  |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------

2_01:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1(local)           |
| LACP (2)           |         1                  |         1(local)           |
| CH Monitor (3)     |         1                  |         1(local)           |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1(local)           |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------

2_02:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1                  |
| LACP (2)           |         1                  |         1                  |
| CH Monitor (3)     |         1                  |         1                  |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1                  |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example output from a Single Site configuration

The SMO task runs on the Security Group Member #1, on which you ran this command (see the string "`(local)`").

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)    |                       Chassis 1                         |
-------------------------------------------------------------------------------
| SMO (0)           |                        1(local)                         |
| General (1)       |                        1(local)                         |
| LACP (2)          |                        1(local)                         |
| CH Monitor (3)    |                        1(local)                         |
| DR Manager (4)    |                        1(local)                         |
| UIPC (5)          |                        1(local)                         |
| Alert (6)         |                        1(local)                         |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Monitoring System and Component Status (asg monitor)

Description

Use the "`asg monitor`" command in Gaia gClish or the Expert mode to monitor continuously the status of the system and its components.

This command shows the same information as the *"Showing Hardware State (asg stat)" on page 264*, but the information stays on the screen and refreshes at intervals specified by the user. Default: 1 second). To stop the monitor session, press **CTRL+C**.

Note - If you run this command in a Virtual System context, you only see the output for that Virtual System. You can also specify the Virtual System context as a command parameter.

Syntax

`asg monitor`
`asg monitor -h`
`asg monitor [-v | -all] [-amw] <Interval>`
`asg monitor -l`

Parameters

Parameter	Description
No Parameters	Shows the Security Group Member status.
`-h`	Shows the built-in help.
`-amw`	Shows the Anti-Malware policy date instead of the Firewall policy date.
`-v`	Shows only the System component status.
`-all`	Shows both Security Group Member and System component status.
`<Interval>`	Configures the data refresh interval (in seconds) for this session. Default is 10 seconds.
`-l`	Shows legend of column title abbreviations.

Examples

Example 1 - Shows the Security Group Member status with the Anti-Malware policy date

```
[Expert@MyChassis-ch0x-0x:0]# asg monitor -amw

-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 12:03:48 hours                                |
| SGMs                        | 2 / 2                                         |
| Version                     | R80.20SP (Build Number XX)                    |
| FW Policy Date              | 21Feb19 14:37                                 |
| AMW Policy Date             | 21Feb19 14:37                                 |
-------------------------------------------------------------------------------
| SGM ID                              Chassis 1                               |
|                                     ACTIVE                                  |
-------------------------------------------------------------------------------
|  1                                    ACTIVE                                |
|  2                                    ACTIVE                                |
-------------------------------------------------------------------------------
```

Example 2 - Shows the Security Group component status

```
[Expert@MyChassis-ch0x-0x:0]# asg monitor -v
Thu Feb 21 21:07:11 IST 2019

-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit        |                      Chassis 1                       | Weight |
-------------------------------------------------------------------------------
| SGMs        |                        2 / 2                         |   6    |
| Ports       |                                                      |        |
|   Standard  |                        8 / 8                         |  11    |
|   Bond      |                        0 / 0                         |  11    |
|   Mgmt      |                        1 / 1                         |  11    |
|   Mgmt Bond |                        0 / 0                         |  11    |
|   Other     |                        0 / 0                         |   6    |
| Sensors     |                                                      |        |
|   SSMs      |                        2 / 2                         |  11    |
|             |                                                      |        |
| Grade       |                      133 / 133                       |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
```

Configuring Alert Thresholds (set chassis alert_threshold)

Description

Use the "`set chassis alert_threshold`" command in Gaia gClish to configure thresholds for performance and hardware alerts.

Syntax to configure alert threshold

```
set chassis alert_threshold <Threshold Name> <Value>
```

Syntax to view an alert threshold configuration

```
show chassis alert_threshold <Threshold Name>
```

Parameters

Parameter	Description
<Threshold Name>	Threshold name as specified in the table below
<Value>	High or low value for the specified threshold

Performance Alert Thresholds

Threshold Name	Scope	Description
`concurr_conn_threshold_high`	Security Group Member	Concurrent connections - High limit
`concurr_conn_threshold_low_ratio`	Security Group Member	Concurrent connections - Low limit (% of the High limit)
`concurr_conn_total_threshold_high`	Security Group	Concurrent connections - High limit
`concurr_conn_total_threshold_low_ratio`	Security Group	Concurrent connections - Low limit (% of the High limit)
`conn_rate_threshold_high`	Security Group Member	Connection rate per second - High limit

Threshold Name	Scope	Description
`conn_rate_threshold_low_ratio`	Security Group Member	Connection rate per second - Low limit (% of the High limit)
`conn_rate_total_threshold_high`	Security Group	Connection rate per second - High limit
`conn_rate_total_threshold_low_ratio`	Security Group	Connection rate per second - Low limit (% of the High limit)
`cpu_load_threshold_perc_high`	Security Group Member	CPU load (%) - High limit
`cpu_load_threshold_perc_low_ratio`	Security Group Member	CPU load (%) - Low limit (% of the High limit)
`hd_util_threshold_perc_high`	Security Group Member	Disk utilization (%) - High limit
`hd_util_threshold_perc_low_ratio`	Security Group Member	Disk utilization (%) - Low limit (% of the High limit)
`mem_util_threshold_perc_high`	Security Group Member	Memory utilization (%) - High limit
`mem_util_threshold_perc_low_ratio`	Security Group Member	Memory utilization (%) - Low limit (% of the High limit)
`packet_rate_threshold_high`	Security Group Member	Packet rate per second - High limit
`packet_rate_threshold_low_ratio`	Security Group Member	Packet rate per second - Low limit (% of the High limit)
`packet_rate_total_threshold_high`	Security Group	Packet rate per second - High limit
`packet_rate_total_threshold_low_ratio`	Security Group	Packet rate per second - Low limit (% of the High limit)
`throughput_threshold_high`	Security Group Member	Throughput (bps) - High limit

Threshold Name	Scope	Description
`throughput_threshold_low_ratio`	Security Group Member	Throughput (bps) - Low limit (% of the High limit)
`throughput_total_threshold_high`	Security Group	Throughput (bps) - High limit
`throughput_total_threshold_low_ratio`	Security Group	Throughput (bps) - Low limit (% of the High limit)

Example - Set the high limit of the memory utilization to 70% of the installed memory

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> set chassis alert_threshold mem_util_threshold_perc_high 70
[Global] MyChassis-ch01-01>
```

Monitoring System Resources (asg resource)

Description

Use the "`asg resource`" command in Gaia gClish or the Expert mode to show this information for Security Group Members:

- RAM and Storage usage and thresholds
- SSD Health

Syntax

`asg resource -h`
`asg resource [-b <SGM IDs>]`
`asg resource --ssd [-v]`

Parameters

Parameter	Description
No Parameters	Shows both the Resource (RAM and Storage) and SSD Health information.
`-h`	Shows the built-in help.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`--ssd [-v]`	Shows only the SSD Health information for all Security Group Members: ■ `--ssd` Shows summary information only (whether it passed the SMART test) ■ `--ssd -v` Shows the summary and verbose information (SSD SMART Attributes)

Examples

Example 1 - Default output

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg resource
+-------------------------------------------------------------------------------------+
|Resource Table                                                                       |
+------------+-------------------------+------------+------------+------------------+
|Member ID   |Resource Name            |Usage       |Threshold   |Total             |
+------------+-------------------------+------------+------------+------------------+
|1_01        |Memory                   |21%         |50%         |62.8G             |
|            |HD: /                    |16%         |80%         |33.9G             |
|            |HD: /var/log             |2%          |80%         |48.4G             |
|            |HD: /boot                |14%         |80%         |288.6M            |
+------------+-------------------------+------------+------------+------------------+
|1_02        |Memory                   |21%         |50%         |62.8G             |
|            |HD: /                    |16%         |80%         |33.9G             |
|            |HD: /var/log             |2%          |80%         |48.4G             |
|            |HD: /boot                |14%         |80%         |288.6M            |
+------------+-------------------------+------------+------------+------------------+
... output is cut for brevity ...
+------------+-------------------------+------------+------------+------------------+
|2_01        |Memory                   |21%         |50%         |62.8G             |
|            |HD: /                    |16%         |80%         |33.9G             |
|            |HD: /var/log             |2%          |80%         |48.4G             |
|            |HD: /boot                |14%         |80%         |288.6M            |
+------------+-------------------------+------------+------------+------------------+
|2_02        |Memory                   |21%         |50%         |62.8G             |
|            |HD: /                    |16%         |80%         |33.9G             |
|            |HD: /var/log             |2%          |80%         |48.4G             |
|            |HD: /boot                |14%         |80%         |288.6M            |
+------------+-------------------------+------------+------------+------------------+
... output is cut for brevity ...
+-----------------------------------------+
|SSD Health                               |
+---------------+-------------------------+
|Member ID      |SMART overall-health     |
+---------------+-------------------------+
|1_01           |PASSED                   |
+---------------+-------------------------+
|1_02           |PASSED                   |
+---------------+-------------------------+
... output is cut for brevity ...
+---------------+-------------------------+
|2_01           |PASSED                   |
+---------------+-------------------------+
|2_02           |PASSED                   |
+---------------+-------------------------+
... output is cut for brevity ...

SSD attributes verifier ended successfully.
[Global] MyChassis-ch01-01>
```

Example 2 - Resource Table for a specific Security Group Member

```
[Expert@MyChassis-ch0x-0x:0]# asg resource -b 1_01
+-------------------------------------------------------------------------------------+
|Resource Table                                                                       |
+-----------+------------------------+------------+------------+--------------------+
|Member ID  |Resource Name           |Usage       |Threshold   |Total               |
+-----------+------------------------+------------+------------+--------------------+
|1_01       |Memory                  |21%         |50%         |62.8G               |
|           |HD: /                   |16%         |80%         |33.9G               |
|           |HD: /var/log            |2%          |80%         |48.4G               |
|           |HD: /boot               |14%         |80%         |288.6M              |
+-----------+------------------------+------------+------------+--------------------+
+-----------------------------------------+
|SSD Health                               |
+---------------+-------------------------+
|Member ID      |SMART overall-health     |
+---------------+-------------------------+
|1_01           |PASSED                   |
+---------------+-------------------------+
|1_02           |PASSED                   |
+---------------+-------------------------+
|1_03           |PASSED                   |
+---------------+-------------------------+
|1_04           |PASSED                   |
+---------------+-------------------------+
|1_05           |PASSED                   |
+---------------+-------------------------+
|2_01           |PASSED                   |
+---------------+-------------------------+
|2_02           |PASSED                   |
+---------------+-------------------------+
|2_03           |PASSED                   |
+---------------+-------------------------+
|2_04           |PASSED                   |
+---------------+-------------------------+
|2_05           |PASSED                   |
+---------------+-------------------------+

SSD attributes verifier ended successfully.
[Expert@MyChassis-ch0x-0x:0]#
```

Example 3 - Verbose SSD Health information

```
[Expert@MyChassis-ch0x-0x:0]# asg resource --ssd -v
+----------------------------------------+
|SSD Health                              |
+---------------+------------------------+
|Member ID      |SMART overall-health    |
+---------------+------------------------+
|1_01           |PASSED                  |
+---------------+------------------------+
|1_02           |PASSED                  |
+---------------+------------------------+
... output is cut for brevity ...
+---------------+------------------------+
|2_01           |PASSED                  |
+---------------+------------------------+
|2_02           |PASSED                  |
+---------------+------------------------+
... output is cut for brevity ...
+-------------------------------------------------------------------------+
|SSD Attributes                                                           |
+------+----------------------------+--------+--------+----------------+
Member 1_01
+------+----------------------------+--------+--------+----------------+
|ID    |Attribute name              |Value   |Trhesh  |Last_failed     |
+------+----------------------------+--------+--------+----------------+
|5     |Reallocated_Sector_Ct       |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
|9     |Power_On_Hours              |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
|12    |Power_Cycle_Count           |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
... output is cut for brevity ...
+------+----------------------------+--------+--------+----------------+
|194   |Temperature_Celsius         |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
... output is cut for brevity ...
+------+----------------------------+--------+--------+----------------+
Member 1_02
+------+----------------------------+--------+--------+----------------+
|ID    |Attribute name              |Value   |Trhesh  |Last_failed     |
+------+----------------------------+--------+--------+----------------+
|5     |Reallocated_Sector_Ct       |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
... output is cut for brevity ...
[Expert@MyChassis-ch0x-0x:0]#
```

Description for the Resource Table section

Column	Description
Member ID	Shows the Security Group Member ID.
Resource Name	Identifies the resource. There are four types of resources: ■ **Memory** ■ **HD** - Hard drive space (/) ■ **HD: /var/log** - Space on hard drive committed to log files ■ **HD: /boot** - Location of the kernel
Usage	Shows the percentage of the resource in use.
Threshold	Indicates the health and functionality of the component. When the value of the resource is greater than the threshold, an alert is sent. You can modify the threshold in Gaia gClish.
Total	Total absolute value in units. For example, the first row shows that `Security Appliance1` on `Chassis1` has 62.8 GB of RAM, and 21% of it are used. An alert is sent, if the usage is greater than 50%.

Description for the SMART Attributes section

Column	Description
SMART overall-health	Shows the state of the SMART test - passed, or failed.
ID	Shows the attribute ID in the decimal format.
Attribute name	Shows the attribute name.
Value	Shows the current value as returned by the SSD. This is a most universal measurement, on the scale from 0 (bad) to some maximum (good) value. Maximum values are typically 100, 200 or 253. The higher the value, the better the SSD health is.
Trhesh	Shows the current threshold. This is the minimum value limit for the attribute. If the value falls below this threshold, the SSD should be checked for errors, and possibly replaced.
Last_failed	Shows when a failure was last reported for this attribute.

Configuring Alerts for Security Group Member and Security Group Events (asg alert)

The "`asg alert`" command is an interactive wizard that configures alerts for Security Group Member and Security Group events.

These events include hardware failure, recovery, and performance-related events. You can create other general events.

An alert is sent when an event occurs. For example, when the value of a hardware resource is greater than the threshold.

The alert message includes the Site ID, Security Group Member ID, and/or unit ID.

The wizard has these options:

Option	Description
Full Configuration Wizard	Creates a new alert.
Edit Configuration	Changes an existing alert.
Show Configuration	Shows existing alert configuration.
Run Test	Runs a test simulation to make sure that the alert works correctly.

To create or change an alert:

Step	Instructions
1	Run in Gaia gClish of a Security Group: `asg alert`
2	Select **Full Configuration Wizard** or **Edit Configuration**.
3	Select and configure these parameters as prompted by the wizard: ■ **SMS** ■ **Email** ■ **SNMP**

SMS Alert Configuration

Parameter	Description
SMS provider URL	Fully qualified URL to your SMS provider.
HTTP proxy and port	Optional. Configure only if the Security Gateway requires a proxy server to reach the SMS provider.
SMS rate limit	Maximum number of SMS messages sent per hour. If there are too many messages, they can be combined together.
SMS user text	Custom prefix for SMS messages.

Email Alert Configuration

Parameter	Description
SMTP server IP	One or more SMTP servers to which the email alerts are sent.
Email recipient addresses	One or more recipient email address for each SMTP server.
Periodic connectivity checks	Tests run periodically to confirm connectivity with the SNMP servers. If there is no connectivity, alert messages are saved and sent in one email when connectivity is restored.
Interval	Interval, in minutes, between connectivity tests.
Sender email address	Email address of the sender for alerts.
Subject	Subject header text for the email alert.
Body text	User defined text for the alert message.

SNMP Alert Configuration

Define one or more SNMP managers to get SNMP traps sent from the Security Gateway.

For each manager, configure these parameters:

Parameter	Description
SNMP manager name	Unique name for the SNMP manager.
SNMP manager IP	IP address of the SNMP Manager (trap receiver).
SNMP version	SNMP version (v2c, v3).
SNMP v3 user name	User name for SNMP v3 authentication.
SNMP v3 security level	Security level for SNMP v3 authentication.
SNMP v3 engine ID	Unique SNMP v3 engine ID used by your system. The default is: `0x80000000010203EA`
SNMP v3 authentication protocol	Authentication protocol (MD5 or SHA) for SNMP v3 authentication.
SNMP v3 authentication password	Authentication password for SNMP v3 authentication.
SNMP v3 privacy protocol	Privacy protocol (DES or AES) for SNMP v3 authentication.
SNMP v3 privacy password	Privacy password for SNMP v3 authentication.
SNMP user text	Custom text for SNMP trap messages.
SNMP community string	Community name.

Notes:

- Based on the settings, some parameters do not appear.
- There are no configurable parameters for log alerts.

System Event Types

```
System event types are:
---------------------------------
1       | SGM State
2       | Chassis State
3       | Port State
4       | Diagnostics
5       | Memory Leak Detection
6       | LSP Monitor Port State Change
7       | VS Monitor State Change
Hardware Monitor events:
8       | Fans
9       | SSM
10      | CMM
11      | Power Supplies
12      | CPU Temperature
Performance events:
13      | Concurrent Connections
14      | Connection Rate
15      | Packet Rate
16      | Throughput
17      | CPU Load
18      | Hard Drive Utilization
19      | Memory Utilization

Please choose event types for which to send alerts: [all]
(format: all or 1,4 or 1,3-7,10)
```

You can select one or more event types:

- One event type.
- A comma-delimited list of more than one event type.
- All event types.

Collecting System Diagnostics (smo verifiers)

In This Section:

Diagnostic Tests

Description

Use the "`smo verifiers`" commands in Gaia gClish to run a specific set of diagnostic tests.

The full set of tests run by default, but you can manually select the tests to run.

The output shows the result of the test, `Passed` or `Failed`, and the location of the output log file.

Syntax

```
show smo verifiers list
      [id <TestId1>,<TestId2>,...]
      [section <SectionName>]
```

```
show smo verifiers report [except]
      [id <TestId1>,<TestId2>,...]
      [name <TestName>]
      [section <SectionName>]
```

```
show smo verifiers print [except]
      [id <TestId1>,<TestId2>,...]
      [name <TestName>]
      [section <SectionName>]
```

```
show smo verifiers
      periodic
      last-run report
      print
```

```
delete smo verifiers purge [save <Num_Logs>]
```

Parameters

Parameter	Description
`list`	Shows the list of tests to run.
`report`	Runs tests and shows a summary of the test results.

Parameter	Description
`print`	Runs tests and shows the full output and summary of the test results.
`except`	Runs all tests except the specified tests. Shows the requested results.
`id <TestId1>,<TestId2>,...`	Specifies the tests by their IDs (comma separated list). To see a list of test IDs, run: `show smo verifiers list`
`name <TestName>`	Specifies the tests by their names. Press the **Tab** key to see a full list of verifiers names.
`section <SectionName>`	Specifies the verifiers section by its name. Press the **Tab** key to see a full list of the existing sections.
`purge`	Deletes the old "`smo verifiers`" logs. Keeps the newest log.
`save <Num_Logs>`	Number of logs to save from the "`smo verifiers`" log files. Default: 5.
`periodic`	Shows the latest `periodic` run results.
`last-run`	Shows the latest run results.

Showing the Tests

The "`show smo verifiers list`" command shows the full list of diagnostic tests.

The list shows the test "`ID`", test "`Title`" (name), and the "`Command`" the "`smo verifiers`" command runs.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers list
-------------------------------------------------------------------------------
| ID | Title              | Command                                          |
-------------------------------------------------------------------------------
| System Components                                                          |
-------------------------------------------------------------------------------
|  1 | System Health      | asg stat -v                                      |
|  2 | Resources          | asg resource                                     |
|  3 | Software Provision | asg_provision                                    |
|  4 | Media Details      | transceiver_verifier -v                          |
|  5 | SSD Health         | asg resource --ssd                               |
-------------------------------------------------------------------------------
| Policy and Configuration                                                   |
-------------------------------------------------------------------------------
|  6 | Distribution Mode  | distutil verify -v                               |
|  7 | DXL Balance        | dxl stat                                         |
|  8 | Policy             | asg policy verify -a                             |
|  9 | AMW Policy         | asg policy verify_amw -a                         |
| 10 | SWB Updates        | asg_swb_update_verifier -v                       |
| 11 | Installation       | installation_verify                              |
| 12 | Security Group     | security_group_util diag                         |
| 13 | Cores Distribution | cores_verifier                                   |
| 14 | Clock              | clock_verifier -v                                |
| 15 | Licenses           | asg_license_verifier -v                          |
| 16 | IPS Enhancement    | asg_ips_enhance status                           |
| 17 | Configuration File | config_verify -v                                 |
-------------------------------------------------------------------------------
| VSX Configuration                                                          |
-------------------------------------------------------------------------------
| 18 | USER KERNEL Dist   | distutil verify_vsx_dist                         |
| 19 | HW Utilization     | hw_utilization -d                                |
| 20 | BMAC VMAC verify   | mac_verifier -x                                  |
-------------------------------------------------------------------------------
| Networking                                                                 |
-------------------------------------------------------------------------------
| 21 | MAC Setting        | mac_verifier -v                                  |
| 22 | ARP Consistency    | asg_arp -v                                       |
| 23 | Bond               | asg_bond -v                                      |
| 24 | IPv4 Route         | asg_route                                        |
| 25 | IPv6 Route         | asg_route -6                                     |
| 26 | Dynamic Routing    | asg_dr_verifier                                  |
| 27 | Local ARP          | asg_local_arp_verifier -v                        |
| 28 | IGMP Consistency   | asg_igmp                                         |
| 29 | PIM Neighbors      | asg_pim_neighbors                                |
-------------------------------------------------------------------------------
| Misc                                                                       |
-------------------------------------------------------------------------------
| 30 | Core Dumps         | core_dump_verifier -v                            |
| 31 | Performance hogs   | asg_perf_hogs                                    |
-------------------------------------------------------------------------------
| Run "show smo verifiers print id <TestNum>" to display test output         |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Showing the Last Run Diagnostic Tests

The "`show smo verifiers last-run report`" command shows the default output for the last run diagnostic tests.

The "`show smo verifiers last-run print`" command shows verbose output for the last run diagnostic tests.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers last-run report
2019-02-07, 01:00:02
-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                  |
|  2 | Resources          | Passed     |                                     |
|  3 | Software Provision | Passed     |                                     |
|  4 | Media Details      | Passed     |                                     |
|  5 | SSD Health         | Passed     | (1)Failed to get SSD overall-health t |
|    |                    |            | est result from Member              |
-------------------------------------------------------------------------------
| Policy and Configuration                                                    |
-------------------------------------------------------------------------------
|  6 | Distribution Mode  | Failed (!) | (1)Verifier error - Check raw output  |
|  7 | DXL Balance        | Passed     |                                     |
|  8 | Policy             | Passed     |                                     |
|  9 | AMW Policy         | Passed     | (1)Not configured                   |
| 10 | SWB Updates        | Passed     | (1)Not configured                   |
| 11 | Installation       | Passed     |                                     |
| 12 | Security Group     | Passed     |                                     |
| 13 | Cores Distribution | Passed     |                                     |
| 14 | Clock              | Passed     |                                     |
| 15 | Licenses           | Failed (!) | (1)Trial license will expire within 2 |
|    |                    |            |  weeks                              |
|    |                    |            | (2)Execution error                  |
| 16 | IPS Enhancement    | Passed     |                                     |
| 17 | Configuration File | Passed     |                                     |
-------------------------------------------------------------------------------
| VSX Configuration                                                           |
-------------------------------------------------------------------------------
| 18 | USER KERNEL Dist   | Failed (!) |                                     |
| 19 | HW Utilization     | Failed (!) | (1)Execution error                  |
| 20 | BMAC VMAC verify   | Passed     |                                     |
-------------------------------------------------------------------------------
| Networking                                                                  |
-------------------------------------------------------------------------------
| 21 | MAC Setting        | Passed     |                                     |
... output was truncated for brevity ...
-------------------------------------------------------------------------------
| Misc                                                                        |
-------------------------------------------------------------------------------
| 30 | Core Dumps         | Failed (!) |                                     |
| 31 | Performance hogs   | Failed (!) |                                     |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 24/31 tests                                                         |
| Run: "show smo verifiers list id 1,6,15,18,19,30,31" to view a complete list |
|  of failed tests                                                            |
| Output file: /var/log/alert_verifier_sum.1-31.2019-02-07_01-00-02.txt       |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Running all Diagnostic Tests

The "`show smo verifiers report`" command runs all diagnostic tests and shows their summary output.

When a test fails, the reasons for failure show in the **Reason** column.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers report
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                  |
|  2 | Resources          | Passed     |                                     |
|  3 | Software Provision | Passed     |                                     |
|  4 | Media Details      | Passed     |                                     |
|  5 | SSD Health         | Passed     | (1)Failed to get SSD overall-health t |
|    |                    |            | est result from Member              |
-------------------------------------------------------------------------------
| Policy and Configuration                                                    |
-------------------------------------------------------------------------------
|  6 | Distribution Mode  | Failed (!) | (1)Verifier error - Check raw output  |
|  7 | DXL Balance        | Passed     |                                     |
|  8 | Policy             | Passed     |                                     |
|  9 | AMW Policy         | Passed     | (1)Not configured                   |
| 10 | SWB Updates        | Passed     | (1)Not configured                   |
| 11 | Installation       | Passed     |                                     |
| 12 | Security Group     | Passed     |                                     |
| 13 | Cores Distribution | Passed     |                                     |
| 14 | Clock              | Passed     |                                     |
| 15 | Licenses           | Failed (!) | (1)Trial license will expire within 2 |
|    |                    |            |  weeks                              |
|    |                    |            | (2)Execution error                  |
| 16 | IPS Enhancement    | Passed     |                                     |
| 17 | Configuration File | Passed     |                                     |
-------------------------------------------------------------------------------
| VSX Configuration                                                           |
-------------------------------------------------------------------------------
| 18 | USER KERNEL Dist   | Failed (!) |                                     |
| 19 | HW Utilization     | Failed (!) | (1)Execution error                  |
| 20 | BMAC VMAC verify   | Passed     |                                     |
-------------------------------------------------------------------------------
| Networking                                                                  |
-------------------------------------------------------------------------------
| 21 | MAC Setting        | Passed     |                                     |
... output was truncated for brevity ...
-------------------------------------------------------------------------------
| Misc                                                                        |
-------------------------------------------------------------------------------
| 30 | Core Dumps         | Failed (!) |                                     |
| 31 | Performance hogs   | Failed (!) |                                     |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 24/31 tests                                                         |
| Run: "show smo verifiers list id 1,6,15,18,19,30,31" to view a complete list |
|  of failed tests                                                            |
| Output file: /var/log/verifier_sum.1-31.2019-02-07_18-35-22.txt             |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Running Specific Diagnostic Tests

These commands run the specified diagnostic tests only:

```
show smo verifiers report name
show smo verifiers report id
```

Syntax to run a test by its name

```
show smo verifiers report name <Test Name>
```

Note - Press the **Tab** key after the "`name`" parameter to see a full list of verifier names.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers report name System_Health
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Passed     |                                     |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 1/1 test                                                            |
| Output file: /var/log/verifier_sum.1.2018-12-10_12-16-51.txt                |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Syntax to run a test by its ID

```
show smo verifiers report id <TestID1>,<TestID2>,...,<TestIDn>
```

Note - To see a list of test IDs, run the "`show smo verifiers list`" command.

Example

This example collects diagnostic information for specified tests 1, 2, and 5.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers report id 1,2,5
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                  |
|  2 | Resources          | Passed     |                                     |
|  5 | SSD Health         | Passed     | (1)Failed to get SSD overall-health t |
|    |                    |            | est result from Member              |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 2/3 tests                                                           |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests  |
| Output file: /var/log/verifier_sum.1-2.5.2019-02-07_18-37-22.txt            |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Collecting Diagnostic Information for a Report Specified Section

The "`show smo verifiers report section`" command runs all diagnostic tests in the specified section.

Syntax

```
show smo verifiers report section <Test Name>
```

Note - Press the **Tab** key after the "`section`" parameter to see a full list of verifier sections.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers report section System_Components
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                               |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                   |
|  2 | Resources          | Passed     |                                      |
|  3 | Software Provision | Passed     |                                      |
|  4 | Media Details      | Passed     |                                      |
|  5 | SSD Health         | Passed     | (1)Failed to get SSD overall-health t |
|    |                    |            | est result from Member               |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 4/5 tests                                                           |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests  |
| Output file: /var/log/verifier_sum.1-5.2019-02-07_18-38-56.txt              |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Error Types

The "`smo verifiers`" command detects these errors:

Error Type	Error	Description
`System health`	`Chassis <X> error`	The Security Group quality grade is less than the defined threshold. We recommend that you correct this issue immediately.
`Hardware`	`<Component> is missing`	The component is not installed in the Chassis. **Note** - This applies only to 60000 / 40000 Appliances.
	`<Component> is down`	The component is installed in the Chassis, but is inactive. **Note** - This applies only to 60000 / 40000 Appliances.
`Resources`	`<Resource> capacity`	The specified resource capacity is not sufficient. You can change the defined resource capacity.
	`<Resource> exceed threshold`	The resource usage is greater than the defined threshold.
`CPU type`	`Non compliant CPU type`	CPU type is not configured in the list of compliant CPUs on at least one Security Group Member. You can define the compliant CPU types.
`Security group`	`<Source> error`	The information collected from this source is different between the Security Group Members.
	`<Sources> differ`	The information collected from many sources is different.

Changing Compliance Thresholds

You can change some compliance thresholds that define a healthy, working system.

Change the threshold values in the `$SMODIR/conf/asg_diag_config` file.

These are the supported resources you can control:

Resource	Instructions
`Memory`	RAM memory capacity in GB
`HD: /`	Disk capacity in GB for *<disk>* - the root (`/`) partition
`HD:/var/log`	Disk capacity in GB for the `/var/log` partition
`HD: /boot`	Disk capacity in GB for the `/boot` partition

Changing the Default Test Behavior of the 'asg diag resource verifier'

By default, the "`asg diag resource verifier`" command only shows a warning about resource mismatches between Security Group Members.

The verification test results show as "`Passed`" in the output and no further action is taken.

You can change the default test behavior:

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `$FWDIR/conf/asg_diag_config` file: `g_all vi $FWDIR/conf/asg_diag_config`
4	Search for this parameter: `MismatchSeverity`

Step	Instructions
5	Set the value of this parameter to one of these values: ■ `fail` Verification test result is set to "`Failed`" ■ `warn` Verification test result is set to "`Passed`", and a warning is shown ■ `ignore` Verification test result is set to "`Ignore`", and no errors are shown
6	Save the changes in the file and exit the editor.

Troubleshooting Failures

Use the "`smo verifiers`" command to troubleshoot a failed diagnostic test.

Example

Below is the example procedure based on the **System Health** test that failed.

1. The **System Health** test failed:

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers report id 1
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                  |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 0/1 test                                                            |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests |
| Output file: /var/log/verifier_sum.1.2019-02-07_20-12-07.txt                |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

2. Print the full report for this failed test:

```
[Global] MyChassis-ch01-01 > show smo verifiers print id 1
==============================
System Health:
==============================


-------------------------------------------------------------------------------
| VSX System Status - Maestro                                                 |
-------------------------------------------------------------------------------
| Up time                     | 06:44:48 hours                                |
| SGMs                        | 3 / 3                                         |
| Virtual Systems             | 1                                             |
| Version                     | R80.20SP (Build Number xxx)                   |
-------------------------------------------------------------------------------
| VS ID:  0                     VS Name:  MyVSname                            |
-------------------------------------------------------------------------------
| SGM ID                              Chassis 1                               |
|                                     ACTIVE                                  |
-------------------------------------------------------------------------------
|  2                                    ACTIVE                                |
|  3                                    ACTIVE                                |
|  4                                    ACTIVE                                |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |                           Chassis 1                        |
-------------------------------------------------------------------------------
| SGMs         |                             3 / 3                          |
| Ports        |                             0 / 0                          |
| SSMs         |                             1 / 2   !                      |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                               |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                   |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 0/1 test                                                            |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests |
| Output file: /var/log/verifier_sum.1.2019-02-07_20-12-14.txt                |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

3. Examine which command produced the failed test:

```
[Global] MyChassis-ch01-01 > show smo verifiers list id 1
-------------------------------------------------------------------------
| ID | Title              | Command                                     |
-------------------------------------------------------------------------
| System Components                                                     |
-------------------------------------------------------------------------
|  1 | System Health      | asg stat -v                                 |
-------------------------------------------------------------------------
| Run "show smo verifiers print id <TestNum>" to display test output    |
-------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

4. Run the applicable command to understand what failed:

```
[Global] MyChassis-ch01-01 > asg stat -v

-------------------------------------------------------------------------------
| VSX System Status - Maestro                                                 |
-------------------------------------------------------------------------------
| Up time                     | 06:45:06 hours                                |
| SGMs                        | 3 / 3                                         |
| Virtual Systems             | 1                                             |
| Version                     | R80.20SP (Build Number xxx)                   |
-------------------------------------------------------------------------------
| VS ID:  0                     VS Name:  MyVSname                            |
-------------------------------------------------------------------------------
| SGM ID                              Chassis 1                               |
|                                     ACTIVE                                  |
-------------------------------------------------------------------------------
|  2                                    ACTIVE                                |
|  3                                    ACTIVE                                |
|  4                                    ACTIVE                                |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit        |                      Chassis 1                        | Weight |
-------------------------------------------------------------------------------
| SGMs        |                        3 / 3                          |   6    |
| Ports       |                                                       |        |
|   Standard  |                        0 / 0                          |  11    |
|   Bond      |                        0 / 0                          |  11    |
|   Other     |                        0 / 0                          |   6    |
| Sensors     |                                                       |        |
|   SSMs      |                        1 / 2   !                      |  11    |
|             |                                                       |        |
| Grade       |                       29 / 40  !                      |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Alert Modes

In This Section:

The Alert Modes are:

- **Enabled** - The system sends an alert for the selected events.
- **Disabled** - The system does not send alerts for the selected events.
- **Monitor** - The system generates a log entry instead of an alert.

Diagnostic Events

Best Practice - Run the "`smo verifiers`" command (or the "`show smo verifiers report`" command) on a regular basis.

If the test fails, an alert appears. The alerts continue to appear in the **Message of the Day** (MOTD) until the issues are resolved.

When the issues are resolved, a **Clear Alert** message appears the next time the test runs.

You can manually run the "`smo verifiers`" command (the "`show smo verifiers report`" command) to confirm the issue is resolved.

Important Notes

- By default, the tests run at 01h:00m each night.

  Changing the default time

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `$FWDIR/conf/asgsnmp.conf` file: `vi $FWDIR/conf/asgsnmp.conf`
4	Change the value in this line: `asg_diag_alert_wrapper`
5	Save the changes in the file and exit the editor.
6	Copy this file to all other Security Group Members: `asg_cp2blades $FWDIR/conf/asgsnmp.conf`

- By default, all tests run.

  Excluding the tests

  Note - When you manually run the "`show smo verifiers report`" command, the complete set of tests runs, even those you excluded.

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Run: `$FWDIR/conf/asg_diag_config`

4	Add this line to the file:
	`excluded_tests=[<Test1>]`
	`[,<Test2>,...]`

5	Save the changes in the file and exit the editor.

6	Copy this file to all other Security Group Members:
	`asg_cp2blades`
	`$FWDIR/conf/asgsnmp.conf`

- All failed tests show in the MOTD.

Excluding failed test notifications from the MOTD

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Run: `# $FWDIR/conf/asg_diag_config`
4	Set the `failed_tests_motd` parameter to `off`
5	Copy this file to all other Security Group Members: `asg_cp2blades $FWDIR/conf/asg_diag_config`
6	Go to Gaia gClish: enter `gclish` and press Enter.
7	Enforce the change: `show smo verifiers report` You can also wait for the next time the "`smo verifiers`" run automatically.

Disabling the MOTD feature

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `$FWDIR/conf/asg_diag_config` file: `vi $FWDIR/conf/asg_diag_config`
4	Set the value of the `motd` parameter to `off`.
5	Save the changes in the file and exit the editor.
6	Copy this file to all other Security Group Members: `asg_cp2blades $FWDIR/conf/asg_diag_config`
7	Go to Gaia gClish: enter `gclish` and press Enter.
8	Enforce the change: `show smo verifiers report` You can also wait for the next time the "`smo verifiers`" run automatically.

Known Limitations of the SMO Verifiers Test

By default, the "`smo verifiers`" command only shows a warning about resource mismatches between Security Group Members.

If the verification test results show **Passed** in the output, no more steps are necessary.

Changing the default behavior

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `$FWDIR/conf/asg_diag_config` file: `vi $FWDIR/conf/asg_diag_config`
4	Search for this parameter: `MismatchSeverity`
5	Set the value of this parameter to one of these values: ■ `fail` Verification test result is set to "`Failed`" ■ `warn` Verification test result is set to "`Passed`", and a warning is shown ■ `ignore` Verification test result is set to "`Ignore`", and no errors are shown
6	Save the changes in the file and exit the editor.
7	Copy this file to all other Security Group Members: `asg_cp2blades $FWDIR/conf/asg_diag_config`

System Monitoring

This section describes features to monitor your system status.

Showing System Serial Numbers (asg_serial_info)

Description

Use the "`asg_serial_info`" command in Gaia gClish or the Expert mode to show the serial numbers of all the Security Group Members in the Security Group.

Syntax

```
asg_serial_info
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_serial_info
Collecting SGMs information...
+-------------------------+
|     Serial numbers      |
+------------+------------+
| Chassis ID |     1      |
| SGM2       | 11xxxxxxxx |
| SGM3       | 12xxxxxxxx |
| SGM4       | 13xxxxxxxx |
+------------+------------+

[Expert@MyChassis-ch0x-0x:0]#
```

Showing the Security Group Version (ver)

Description

Use the "`ver`" command in Gaia gClish to show the Security Group software version.

Syntax

```
ver
```

Example

```
[Global] MyChassis-ch01-01 > ver
1_01:
Product version Check Point Gaia R80.20SP
OS build xxx
OS kernel version 3.10.0-693cpx86_64
OS edition 64-bit

1_02:
Product version Check Point Gaia R80.20SP
OS build xxx
OS kernel version 3.10.0-693cpx86_64
OS edition 64-bit

[Global] MyChassis-ch01-01 >
```

Showing System Messages (show smo log)

Description

Use the "`show smo log`" command in Gaia gClish to show the output of log files aggregated from all Security Group Members.

The output shows log files in a chronological sequence.

Each line shows the Security Group Member that created the log entry.

Syntax

```
show smo log <Log File> [from <Date>] [to <Date>] [tail <N>]
[filter <String>]
```

Parameters

Parameter	Description
`tail <N>`	Show only the last `n` lines of the log file for each Security Group Member. For example, `tail 3` shows only the last three lines of the specified log file.
<Log File>	Enter the name of the common log file or the full path of the file.
`from <Date>`	Shows only the log from a given date and above.
`to <Date>`	Shows only the log until the given date.
`filter <String>`	Word or phrase to use as an output filter. For example, `filter ospf` shows only OSPF messages.

Example

This example shows messages on Site 1 that contain the word "`Restarted`":

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo log messages filter Restarted
Feb 5 12:40:07 1_03 MyChassis-ch01-03 pm[8465]: Restarted /bin/routed[8489], count=1
Feb 5 12:40:09 1_04 MyChassis-ch01-04 pm[8449]: Restarted /bin/routed[9995], count=1
Feb 5 12:40:09 1_04 MyChassis-ch01-04 pm[8449]: Restarted /opt/CPsuite-R80.20/fw1/bin/cmd[11291], count=1
Feb 5 12:40:09 1_04 MyChassis-ch01-04 pm[8449]: Restarted /usr/libexec/gexecd[11292], count=1
Feb 5 12:40:10 1_03 MyChassis-ch01-03 pm[8465]: Restarted /usr/libexec/gexecd[9701], count=1
Feb 5 12:40:10 1_03 MyChassis-ch01-03 pm[8465]: Restarted /bin/routed[11328], count=2
Feb 5 12:40:10 1_05 MyChassis-ch01-05 pm[8458]: Restarted /bin/routed[9734], count=1
Feb 5 12:40:10 1_05 MyChassis-ch01-05 pm[8458]: Restarted /usr/libexec/gexecd[11331], count=1
Feb 5 12:40:11 1_01 MyChassis-ch01-01 pm[8463]: Restarted /bin/routed[12253], count=3
Feb 5 12:40:11 1_04 MyChassis-ch01-04 pm[8449]: Restarted /bin/routed[11378], count=2
Feb 5 12:40:11 1_04 MyChassis-ch01-04 pm[8449]: Restarted /opt/CPsuite-R80.20/fw1/bin/cmd[11379], count=2
[Global] MyChassis-ch01-01 >
```

Configuring a Dedicated Logging Port

The logging mechanism on each Security Group Member in Security Groups forwards the logs directly to a dedicated Log Server over the Quantum Maestro Orchestrator's management port assigned to this Security Group.

However, the Quantum Maestro Orchestrator's management ports can experience a high load when Security Group Members generate a large number of logs.

To reduce the load on the Quantum Maestro Orchestrator's management ports:

1. Assign a dedicated Quantum Maestro Orchestrator port of type `management` to a Security Group for logging
2. Configure the Security Group to send the logs to the dedicated Log Server

Topology:

```
[Management Server](some interface) <===> (management port 1 on Quantum Maestro Orchestrator)[Security Group]
```

```
[Management Server](some interface) <===> (interface 1) [Log Server] (interface 2) <===> (management port 2 on Quantum Maestro Orchestrator)[Security Group]
```

Procedure:

Step	Instructions
1	Install a dedicated Log Server: a. Install a dedicated Log Server with two physical interfaces. See the applicable *Installation and Upgrade Guide* > Chapter *Installing a Dedicated Log Server or SmartEvent Server.* b. Connect one physical interface on the dedicated Log Server to the Management Server. c. Connect another physical interface on the dedicated Log Server directly to an available management port on the Quantum Maestro Orchestrator. **Important** - Do **not** use the same port on the Quantum Maestro Orchestrator, which connects to the Management Server. d. In SmartConsole, create the required object that represents the dedicated Log Server. See the applicable *Installation and Upgrade Guide* > Chapter *Installing a Dedicated Log Server or SmartEvent Server.*
2	On the Quantum Maestro Orchestrator, assign the dedicated port of type `management` to a Security Group and apply the changes.

Step	Instructions

3	In the Gaia OS of the Security Group, configure in Gaia gClish the dedicated management port.
	Syntax:
	`[Expert@MyChassis-ch0x-0x:0]# gclish`
	`[Global] MyChassis-ch01-01> set interface ethX-MgmtY ipv4-address <IPv4 Address> mask-length <Mask Length>`
	Example:
	`[Global] MyChassis-ch01-01 > set interface eth1-Mgmt2 ipv4-address 2.2.2.10 mask-length 24`
	Note - You must assign an IPv4 address from the same subnet as assigned to the dedicated interface on the Log Server, which connects to the Quantum Maestro Orchestrator.

4	In SmartConsole, configure the Security Group object to send its logs to the dedicated Log Server. See the applicable *Logging and Monitoring Administration Guide* > Chapter *Getting Started* > Section *Deploying Logging Section* - Subsection *Configuring the Security Gateways for Logging*.

Note - The SMO makes sure that return traffic from the Log Server reaches the correct Security Group Member in the Security Group.

Log Server Distribution (asg_log_servers, set / show smo log-distribution)

Description

In SmartConsole, you can configure multiple Log Servers for each Security Gateway object.

In this environment, the Security Gateway sends its logs to all of its configured Log Servers.

Each Security Group Member sends its logs to all Log Servers in the configuration.

To reduce the load on the Log Servers, enable the distribution of different Log Servers to different Security Groups.

When enabled, each Security Group Member sends its logs to one Log Server only.

Note - You cannot configure the Security Group Member to send its logs to a specific Log Server. Distribution is automatic.
The Security Group automatically decides which Log Server is assigned to which Security Group Member.

Syntax in the R80.20SP Jumbo Hotfix Accumulator Take 105 and above

Run these commands in Gaia gClish.

- To work with the distribution of existing Log Servers between Security Group Members:
  - To enable (`on`) or disable (`off`) the distribution mode for Log Servers:

    ```
    set smo log-distribution log-server state {on | off}
    ```

  - To view the distribution mode state for Log Servers:

    ```
    show smo log-distribution log-server state
    ```

  - To view which Log Servers are assigned to Security Group Members:

    ```
    show smo log-distribution log-server distribution
    ```

- To work with the distribution of existing Alert Servers between Security Group Members:

- To enable (`on`) or disable (`off`) the distribution mode for Alert Servers:

```
set smo log-distribution alert-server state {on | off}
```

- To view the distribution mode state for Alert Servers:

```
show smo log-distribution alert-server state
```

- To view which Alert Servers are assigned to Security Group Members:

```
show smo log-distribution alert-server distribution
```

Syntax in R80.20SP without the R80.20SP Jumbo Hotfix Accumulator

Important - This command is **not** supported on a Security Group in the VSX mode (Known Limitation MBS-6306).

Run this command in Gaia gClish or the Expert mode.

```
asg_log_servers
```

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_log_servers

+------------------------------------------------+
|             Log Servers Distribution           |
+------------------------------------------------+
Log Servers Distribution Mode: Disabled

Available Log Servers:
* logServer
* Gaia
* LogServer2

Logs will be sent to all available servers.

Choose one of the following options:
-----------------------------------
1) Configure Log Servers Distribution mode
2) Exit

 >1
+------------------------------------------------+
|             Log Servers Distribution           |
+------------------------------------------------+

Log Servers Distribution Mode: Disabled

Choose the desired option:
--------------------------
1) Enable Log Servers Distribution mode
2) Disable Log Servers Distribution mode
3) Back
```

If Log Servers Distribution is already enabled, the command shows which Log Servers are assigned to each Security Group Member:

```
+-----------------------------------------------+
|             Log Servers Distribution          |
+-----------------------------------------------+

Log Servers Distribution Mode: Enabled

Available Log Servers:
* LogServer
* Gaia
* LogServer2

Log Servers Distribution:

+-----------------------------------+
| Blade id |        Chassis 1       |
|-----------------------------------|
|    1     |  Gaia                  |
|    2     |  LogServer2            |
|    3     |  LogServer             |
|    4     |  Gaia                  |
|    5     |  -                     |
|    6     |  LogServer             |
|    7     |  -                     |
|    8     |  -                     |
|    9     |  LogServer             |
|    10    |  Gaia                  |
|    11    |  LogServer2            |
|    12    |  -                     |
+-----------------------------------+

("-" - Blade is not in Security Group)

Choose one of the following options:
-----------------------------------
1) Configure Log Servers Distribution mode
2) Exit
```

Command Auditing (asg log audit)

Use the CLI command auditing to:

- Notify users about critical actions they are about to do
- Obtain confirmation for critical actions
- Create forensic logs

If users confirm the action, it is necessary to supply their names and provide a reason for running the command.

If the command affects a Critical Device (Pnote), a second confirmation can be required.

For example, if you use administrative privileges to change the state of a Security Group Member to DOWN, the output looks like this:

```
[Expert@MyChassis-ch0x-0x:0]# asg_sgm_admin -b 2_01 down
You are about to perform sgm_admin down on blades: 2_01

Are you sure? (y - yes, any other key - no) y

sgm_admin down requires auditing
Enter your full name: John Smith
Enter reason for sgm_admin down [Maintenance]: Maintenance
WARNING: sgm_admin down on SGM: 2_01, User: John Smith, Reason: Maintenance
```

Description

Use the "`asg log audit`" command to see the audit logs.

Syntax

```
asg log audit
```

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg log audit
Aug 11 14:14:21 2_01 WARNING: Chassis admin-state up on chassis: 1, User: johnsmith, Reason: Maintenance
Aug 11 16:45:15 2_01 WARNING: Reboot on blades: 1_01,1_02,1_03,1_04,1_05,2_02,2_03,2_04,2_05, User: johnsmith, Reason: Maintenance
Aug 18 14:28:57 2_01 WARNING: Chassis admin-state down on chassis: 2, User: johnsmith, Reason: Maintenance
Aug 18 14:31:08 2_01 WARNING: Chassis admin-state up on chassis: 1, User: Peter, Reason: Maintenance
Aug 18 14:32:32 2_01 WARNING: Chassis admin-state down on chassis: 2, User: O, Reason: Maintenance
Aug 20 15:38:58 2_01 WARNING: Blade_admin down on blades: 2_02,2_03,2_04,2_05, User: Paul, Reason: Maintenance
Aug 21 10:00:05 2_01 CRITICAL: Reboot on blades: all, user: ms, Reason: Maintenance
[Expert@MyChassis-ch0x-0x:0]#
```

Viewing a Log File (asg log)

Description

Use the "`asg log`" command in the Expert mode to see the contents of a specified log file.

Syntax

```
asg log [-b <SGM IDs>] --file <Log File> [--from "<Timestamp>"] [--to "<Timestamp>"] [--tail <N>] [--filter <String>]
```

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)

Parameter	Description
<Log File>	Specifies the log file by its type or full path: ■ `audit` If you specify the log type, the output shows all audit logs in the `/var/log/` directory. To specify a log file, enter its full path and name. For example: `/var/log/asgaudit.log.1` ■ `ports` If you specify the log type, the output shows all ports logs in the `/var/log/` directory. To specify a log file, enter its full path and name. For example: `/var/log/ports` ■ `dist_mode` If you specify the log type, the output shows all logs for the Distribution Mode activity. To specify a log file, enter its full path and name. For example: `/var/log/dist_mode` See *"Working with the Distribution Mode" on page 159*.
`--from "`*<Timestamp>*`"`	Shows only the log entries from the specified timestamp and above. You must use the timestamp as it appears in the log file.
`--to "`*<Timestamp>*`"`	Shows only the log entries until the specified timestamp. You must use the timestamp as it appears in the log file.
`--tail <`*N*`>`	Show only the last `N` lines of the log file for each Security Group Member. For example, "`-tail 3`" shows only the last 3 lines of the specified log file. Default: 10 lines.
`--filter <`*String*`>`	Specifies a text string to use as a filter for the log entries. For example: `--filter debug`

Examples

Example 1 - Audit logs (specified by the log type)

```
[Expert@MyChassis-ch0x-0x:0]# asg log --file audit
Feb 02 17:36:12 1_01 WARNING: Blade_admin up on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:16:17 1_01 WARNING: Blade_admin down on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:17:40 1_01 WARNING: Blade_admin up on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:19:53 1_01 WARNING: Blade_admin down on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:22:33 1_01 WARNING: Blade_admin up on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:23:30 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04_05, User: y, Reason: y
Feb 03 08:38:16 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 09:21:09 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 11:07:08 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 11:16:56 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 11:33:10 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 11:50:08 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 13:32:32 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 14:30:26 1_01 WARNING: Reset sic on blades: all, User: johndoe, Reason: test
Feb 03 14:48:03 1_01 WARNING: Reset sic on blades: all, User: johndoe, Reason: test
Feb 03 15:34:11 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 17:55:23 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2 - Port logs (specified by the log type), last 12 lines

```
[Expert@MyChassis-ch0x-0x:0]# asg log --file ports -tail 12
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-09 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-10 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-11 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-12 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-13 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-14 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-15 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-16 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-Mgmt1 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-Mgmt2 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-Mgmt3 link is down
Feb 3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-Mgmt4 link is down
[Expert@MyChassis-ch0x-0x:0]#
```

Example 3 - Port logs (specified by the full path), filtered by timestamps

```
[Expert@MyChassis-ch0x-0x:0]# asg log --file /var/log/ports --from "Feb 21 17:28:41 2019" --to "Feb 21 17:28:41 2019"
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-Mgmt1, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-57, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-59, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-61, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-63, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-57, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-59, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-61, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-63, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 MyChassis-ch01-02 cphaprob: Link state command ended successfully
[Expert@MyChassis-ch0x-0x:0]#
```

Example 4 - Distribution Mode logs (specified by the log type), filtered by the string "bridge"

```
[Expert@MyChassis-ch0x-0x:0]# asg log -b 1_01,1_04 --file dist_mode -f bridge
Feb 2 18:10:30 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:10:30 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:12:31 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:12:31 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:14:14 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:14:14 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:14:30 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:14:30 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:16:19 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
[Expert@MyChassis-ch0x-0x:0]#
```

Monitoring Virtual Systems (cpha_vsx_util monitor)

Description

Use the "`cpha_vsx_util monitor`" command in the Expert mode to stop or start monitoring of Virtual Systems.

The state of a Security Group Member is **not** affected by non-monitored Virtual Systems. For example, a non-monitored Virtual System in a problem state is ignored - the Security Group Member state does **not** change to DOWN.

Use Case

A Virtual System that is not monitored is useful, if it is necessary for the Security Group Member to be in the UP state, even if a specific Virtual System is DOWN or does not have a Security Policy (for example, after you unload the local policy).

Syntax

```
cpha_vsx_util monitor show
cpha_vsx_util monitor {start | stop} <VS IDs>
```

Parameters

Parameter	Description
`show`	Shows all non-monitored Virtual Systems.
`stop`	Stops the monitoring of the specified Virtual Systems. **Important** - When you stop the monitoring of a Virtual System, you must run the "`cpha_vsx_util monitor start <VS IDs>`" command to start it again. Monitoring does not start automatically after a reboot.
`start`	Starts the monitoring of the specified Virtual Systems.

Parameter	Description
`<VS IDs>`	Applies to Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.

Software Blades Update Verification (asg_swb_update_verifier)

Description

Use the "`asg_swb_update_verifier`" command in Gaia gClish or Expert mode to make sure that the signatures are up-to-date for these Software Blades:

- Anti-Virus
- Anti-Bot
- Application Control
- URL Filtering

Syntax

```
asg_swb_update_verifier [-v] [-b <SGM IDs> [-m <Product>] [-n [-p
<IP Address>:<Port>]] ] [-u <Product>]
```

Parameters

Parameter	Description
`-v`	Shows verbose output.

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`)
`-m <Product>`	Forces a manual update for the specified Software Blades on the Security Group Members specified with the "`-b <SGM IDs>`" parameter. Valid values: ■ `all` All applicable Software Blades ■ `Anti-Bot` The Anti-Bot Software Blade ■ `Anti-Virus` The Anti-Virus Software Blade ■ `APPI` The Application Control Software Blade ■ `URLF` The URL Filtering Software Blade
`-n`	Forces an update download from the Internet. Use with the "`-m`" parameter.
`-p <IP Address>:<Port>`	Forces an update download from the Internet and uses the specified HTTP proxy. Use with the "`-m`" parameter. ■ `<IP Address>` - IP address of the HTTP proxy server ■ `<Port>` - TCP port to use on the HTTP proxy server

Parameter	Description
`-u <Product>`	Forces a database update for the specified Software Blades. Valid values: ■ `all` All applicable Software Blades ■ `Anti-Bot` The Anti-Bot Software Blade ■ `Anti-Virus` The Anti-Virus Software Blade ■ `APPI` The Application Control Software Blade ■ `URLF` The URL Filtering Software Blade

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg_swb_update_verifier
+-------------------------------------------------------------------------------+
| product    | sgm  | status           | DB version | next update check        |
+-------------------------------------------------------------------------------+
| APPI       | 2_01 | failed           | 14061202   | Thu Jun 12 10:32:55 2014 |
| APPI       | 2_02 | failed           | 14061202   | Thu Jun 12 10:32:41 2014 |
| Anti-Bot   | 2_01 | up-to-date       | 1405220911 | Thu Jun 12 09:28:34 2014 |
| Anti-Bot   | 2_02 | up-to-date       | 1405220911 | Thu Jun 12 09:28:45 2014 |
| Anti-Virus | 2_01 | up-to-date       | 1406121233 | Thu Jun 12 09:28:12 2014 |
| Anti-Virus | 2_02 | new              | 1406121234 | Thu Jun 12 09:28:10 2014 |
| URLF       | 2_01 | not-installed    | N/A        | N/A                      |
| URLF       | 2_02 | not-installed    | N/A        | N/A                      |
+-------------------------------------------------------------------------------+

Report:
------------------------------ APPI ------------------------------------------
DB versions verification                                          [   OK   ]
statuses verification                                            [ FAILED ]

------------------------------ URLF ------------------------------------------
DB versions verification                                          [   OK   ]
statuses verification                                            [   OK   ]

------------------------------ Anti-Bot --------------------------------------
DB versions verification                                          [   OK   ]
statuses verification                                            [   OK   ]

------------------------------ Anti-Virus ------------------------------------
DB versions verification                                          [   OK   ]
statuses verification                                            [   OK   ]
[Global] MyChassis-ch01-01 >
```

Output description

Field	Description
product	Name of the Software Blade.
sgm	Security Group Member ID.
status	Update status.
DB version	Database version for a Software Blade.
next update check	Date and time for the next automatic update.
DB versions verification	■ **OK** - The database version is correct. ■ **FAILED** - The database version is incorrect.
statuses verification	■ **OK** - The update installed correctly or no update is needed. ■ **FAILED** - The update did not install correctly.

Working with SNMP

You can use SNMP to monitor different aspects of Quantum Maestro Orchestrators and Security Groups.

Monitoring Quantum Maestro Orchestrators over SNMP

In This Section:

You can use SNMP to monitor different aspects of the Quantum Maestro Orchestrator:

- Software versions
- Key performance indicators

Note - Hardware monitoring is not supported..

Enabling SNMP Monitoring on Quantum Maestro Orchestrators

Step	Instructions
1	Upload these Check Point MIB files from the Quantum Maestro Orchestrator to your third-party SNMP monitoring software: ■ The SNMP MIB file: `$CPDIR/lib/snmp/chkpnt.mib` ■ The SNMP Trap MIB file: `$CPDIR/lib/snmp/chkpnt-trap.mib`
2	Connect to the command line on the Quantum Maestro Orchestrator.
3	Log in to Gaia Clish.

4	Enable the Gaia SNMP Agent:
	`set snmp agent on`
	`save config`

Supported SNMP OIDs for Quantum Maestro Orchestrators

Only these branches are supported:

Branch	OID	
svn	Numerical	.1.3.6.1.4.1.2620.1.6
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.svn
mngmt	Numerical	.1.3.6.1.4.1.2620.1.7
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.mngmt

Supported SNMP Trap OIDs for Quantum Maestro Orchestrators

Only these branches are supported:

Branch	OID	
chkpntTrapInfo	Numerical	.1.3.6.1.4.1.2620.1.2000.0
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapInfo
chkpntTrapNet	Numerical	.1.3.6.1.4.1.2620.1.2000.1
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapNet
chkpntTrapDisk	Numerical	.1.3.6.1.4.1.2620.1.2000.2
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapDisk
chkpntTrapCPU	Numerical	.1.3.6.1.4.1.2620.1.2000.3
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapCPU
chkpntTrapMemory	Numerical	.1.3.6.1.4.1.2620.1.2000.4
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapMemory

Notes:

- The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.
- The "`set snmp traps`" command is not supported.

Monitoring Security Groups over SNMP

In This Section:

You can use SNMP to monitor different aspects of the Security Group, including:

- Software versions
- Hardware status
- Key performance indicators
- High Availability status

Enabling SNMP Monitoring of Security Groups

Step	Instructions
1	Upload these Check Point MIB files from a Security Group Member in the applicable Security Group to your third-party SNMP monitoring software: ■ The SNMP MIB file: `$CPDIR/lib/snmp/chkpnt.mib` ■ The SNMP Trap MIB file: `$CPDIR/lib/snmp/chkpnt-trap.mib`
2	Connect to the command line on the Security Group.
3	Log in to Gaia Clish.
4	Go to Gaia gClish: enter `gclish` and press Enter.

5	Enable the Gaia SNMP Agent:
	`set snmp agent on`
	`save config`

Supported SNMP OIDs for Security Groups

Only this branches is supported:

Branch	OID	
`asg`	Numerical	`1.3.6.1.4.1.2620.1.48`
	Full Text	`.iso.org.dod.internet.private.enterprise.checkpoint.products.asg`

Supported SNMP Trap OIDs for Security Groups

Only this SNMP Trap is supported:

Branch	OID	
`asgTrap`	Numerical	`1.3.6.1.4.1.2620.1.2001`
	Full Text	`.iso.org.dod.internet.private.enterprise.checkpoint.products.asgTrap`

Notes:

- The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.
- The "`set snmp traps`" command is not supported.
  You must use the "`asg alert`" configuration wizard for this purpose.
  See *"Configuring Alerts for Security Group Member and Security Group Events (asg alert)" on page 286*.

SNMP Monitoring of Security Groups in VSX Mode

For more information, see the:

- *R80.20SP Quantum Maestro Gaia Administration Guide*
- *R80.20SP Quantum Maestro VSX Administration Guide*
- sk90860: How to configure SNMP on Gaia OS

Common SNMP OIDs for Security Groups

This table shows frequently used SNMP OIDs that are applicable to Security Groups:

Name	Type	Numerical OID	Comments
System Throughput	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.1 IPv6: .1.3.6.1.4.1.2620.1.48.21.1	
System Connection Rate (connections per second)	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.2 IPv6: .1.3.6.1.4.1.2620.1.48.21.2	
System Packet Rate (packet per second)	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.3 IPv6: .1.3.6.1.4.1.2620.1.48.21.3	
System Concurrent Connections	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.4 IPv6: .1.3.6.1.4.1.2620.1.48.21.4	
System Accelerated Connections Per Second	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.6 IPv6: .1.3.6.1.4.1.2620.1.48.21.6	
System non-accelerated Connections Per Second	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.7 IPv6: .1.3.6.1.4.1.2620.1.48.21.7	
System Accelerated Concurrent Connections	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.8 IPv6: .1.3.6.1.4.1.2620.1.48.21.8	
System Non-accelerated Concurrent Connections	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.9 IPv6: .1.3.6.1.4.1.2620.1.48.21.9	

Name	Type	Numerical OID	Comments
System CPU load - average	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.10 IPv6: .1.3.6.1.4.1.2620.1.48.21.10	
System Acceleration CPU load - average	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.11 IPv6: .1.3.6.1.4.1.2620.1.48.21.11	
System FW instances load - average	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.14 IPv6: .1.3.6.1.4.1.2620.1.48.21.14	
System VPN Throughput	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.17 IPv6: .1.3.6.1.4.1.2620.1.48.21.17	
System Path distribution (fast, medium, slow, drops)	Table	IPv4: .1.3.6.1.4.1.2620.1.48.20.24 IPv6: .1.3.6.1.4.1.2620.1.48.21.24	Path distribution of: ■ throughput ■ pps ■ cps ■ concurrent connections
Per-Security Group Member counters	Table	IPv4: .1.3.6.1.4.1.2620.1.48.20.25 IPv6: .1.3.6.1.4.1.2620.1.48.21.25	Counters of: ■ throughput ■ cps ■ pps ■ concurrent connections ■ SecureXL CPU usage (avg / min / max) ■ Firewall CPU usage (avg / min / max)

Name	Type	Numerical OID	Comments
Performance peaks	Table	IPv4: .1.3.6.1.4.1.2620.1.48.20.26 IPv6: .1.3.6.1.4.1.2620.1.48.21.26	
Resources on every Security Group Member	Table	1.3.6.1.4.1.2620.1.48.23	Memory and Hard Disk utilization
CPU Utilization on every Security Group Member	Table	1.3.6.1.4.1.2620.1.48.29	

System Optimization

This section describes some optimization steps you can take.

Configuring Services to Synchronize After a Delay

Some TCP services (for example, HTTP) are characterized by connections with a very short duration. There is no point to synchronize these connections, because every synchronized connection consumes resources on the Security Group, and the connection is likely to have finished by the time an internal failover occurs.

For short-lived services, you can use the *Delayed Notifications* feature to delay telling the Security Group about a connection, so that the connection is only synchronized, if it still exists X seconds (by default, 3 seconds) after the connection was initiated. The Delayed Notifications feature requires SecureXL to be enabled on the Security Group (this is the default).

Notes:

- By default, a connection is synchronized to backup Security Group Members only if it exists for more than 3 seconds.
- Asymmetric connections are synchronized to backup Security Group Members on the Active Site, if according to the DXL calculation, the Client-to-Server connection and the Server-to-Client connection are passing through different Security Group Members.

To control the "Delayed Notifications" feature:

- To **enable** this feature (this is the default):
  1. Connect to the command line on the Security Group.
  2. Log in to the Expert mode.
  3. Run:
     - To enable temporarily in the current session, if you disabled it earlier (does not survive reboot):

       ```
       g_fw ctl set int fw_cluster_use_delay_sync 1
       ```

     - To enable permanently, if you disabled it earlier (survives reboot):

       ```
       g_update_conf_file fwkern.conf fw_cluster_use_delay_
       sync=1
       ```

- To **disable** this feature (this increases the CPU load):
  1. Connect to the command line on the Security Group.
  2. Log in to the Expert mode.
  3. Run:
     - To disable temporarily in the current session (does not survive reboot):

       ```
       g_fw ctl set int fw_cluster_use_delay_sync 0
       ```

     - To disable permanently (survives reboot):

       ```
       g_update_conf_file fw_cluster_use_delay_sync=0
       ```

To configure an applicable delay:

1. In SmartConsole, click **Objects > Object Explorer**.
2. In the left tree, click the small arrow on the left of the **Services** to expand this category.
3. In the left tree, select **TCP**.
4. Search for the applicable TCP service.
5. Double-click the applicable TCP service.
6. In the TCP service properties window, click **Advanced** page.
7. At the top, select **Override default settings**.

   On Domain Management Server, select **Override global domain settings**.
8. At the bottom, in the **Cluster and synchronization** section:
   a. Select **Synchronize connections on cluster if State Synchronization is enabled on the cluster**.
   b. Select **Start synchronizing**.
   c. Enter the applicable value.

   Important - This change applies to all policies that use this service.
9. Click **OK**.
10. Close the **Object Explorer**.
11. Publish the SmartConsole session.
12. Install the Access Control Policy on the Scalable Platform Security Gateway object.

Note - The Delayed Notifications setting in the service object is ignored, if Connection Templates are not offloaded by the Firewall to SecureXL. For additional information about the Connection Templates, see the *R80.20SP Quantum Maestro Performance Tuning Administration Guide*.

Firewall Connections Table Size for VSX Gateway

You can configure the limit for the Firewall Connections table on Virtual Systems:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Virtual System.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the Virtual System object.
4	From the left tree, click **Optimizations**.
5	In the **Calculate the maximum limit for concurrent connections** section, select **Manually**.
6	Enter or select a value.
7	Click **OK**.
8	Install the Access Control Policy on the Virtual System object.

Forwarding specific inbound-connections to the SMO (asg_excp_conf)

You can configure the Security Group to forward specific inbound connections to the SMO Security Group Member.

Important:

- This command supports only IPv4 connections.
- This command does not support local outgoing connections that the Security Group initiates.
- In VSX mode, you must run this command in the context of the applicable Virtual System.
- This command supports a maximum of 15 exceptions (in VSX mode, this limit is global for all Virtual Systems).
- These exceptions are saved in the `$FWDIR/tmp/tmp_exception_entries.txt` file (IPv4 addresses are converted to a special format).

Syntax

```
asg_excp_conf
      clear
      del <ID>
      get
      set <type> <src_ip> <sport> <dst_ip> <dport>
```

Parameters

Parameter	Description
`clear`	Clears the table with all exception entries.
`del <ID>`	Deletes a specific exception entry by its ID. Use the "`get`" parameter to see the IDs. ID numbers start from 0 (zero).
`get`	Shows the table with all exception entries.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><code>set <type> <src_ip> <sport> <dst_ip> <dport></code></td><td>
Configures a new exception entry.
Notes:

This command does not support wildcard characters (<code>*</code> or <code>?</code>) or the word "<code>any</code>".
You must always configure the exact values of the connection 4-tuple.
The order of these arguments is predefined (for example, "<code><src_ip></code>" is always the second argument).

Arguments:

<code><type></code>
Configures the match condition - which connection parameters the Security Group must consider.
Although you configure all connection parameters, the Security Group uses only specific parameters determined by the <code><type></code> value.
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>1</td><td>Match the inbound connection by the source IPv4 address only</td></tr>
<tr><td>2</td><td>Match the inbound connection by the destination IPv4 address only</td></tr>
<tr><td>3</td><td>Match the inbound connection by the source port only</td></tr>
<tr><td>4</td><td>Match the inbound connection by the destination port only</td></tr>
<tr><td>5</td><td>Match the inbound connection by all these parameters:
source IPv4 address
destination IPv4 address</td></tr>
<tr><td>6</td><td>Match the inbound connection by all these parameters:
source IPv4 address
source port</td></tr>
</table>

</td></tr>
</table>

Parameter	Description
	<table><tr><th>Value</th><th>Description</th></tr><tr><td>7</td><td>Match the inbound connection by all these parameters: - source IPv4 address - destination port </td></tr><tr><td>8</td><td>Match the inbound connection by all these parameters: - source port - destination IPv4 address </td></tr><tr><td>9</td><td>Match the inbound connection by all these parameters: - destination IPv4 address - destination port </td></tr><tr><td>10</td><td>Match the inbound connection by all these parameters: - source port - destination port </td></tr><tr><td>11</td><td>Match the inbound connection by all these parameters: - source IPv4 address - source port - destination IPv4 address </td></tr><tr><td>12</td><td>Match the inbound connection by all these parameters: - source IPv4 address - destination IPv4 address - destination port </td></tr><tr><td>13</td><td>Match the inbound connection by all these parameters: - source IPv4 address - source port - destination port </td></tr></table>

Parameter	Description
	<table><tr><th>Value</th><th>Description</th></tr><tr><td>14</td><td>Match the inbound connection by by all these parameters: - source port - destination IPv4 address - destination port </td></tr><tr><td>15</td><td>Match the inbound connection by all these parameters: - source IPv4 address - source port - destination IPv4 address - destination port </td></tr></table> <*src_ip*> Configures the Source IPv4 address <*sport*> Configures the Source port <*dst_ip*> Configures the Destination IPv4 address <*dport*> Configures the Destination port

Examples

asg_excp_conf set

```
[Expert@HostName-ch0x-0x:0] asg_excp_conf set 2 192.168.20.30
40000 172.16.40.50 80
1_01:
Exception entry added successfuly.
1_02:
Exception entry added successfuly.
1_03:
Exception entry added successfuly.
1_04:
Exception entry added successfuly.
2_01:
Exception entry added successfuly.
2_02:
Exception entry added successfuly.
2_03:
Exception entry added successfuly.
2_04:
Exception entry added successfuly.
[Expert@HostName-ch0x-0x:0]
```

asg_excp_conf get

```
[Expert@HostName-ch0x-0x:0] asg_excp_conf get
1_01:
-------------------------------------------------
Exceptions table: ---------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
-------------------------------------------------------------
-------------------------------------------------------------
1_02:
-------------------------------------------------
Exceptions table: ---------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
-------------------------------------------------------------
-------------------------------------------------------------
1_03:
-------------------------------------------------
Exceptions table: ---------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
-------------------------------------------------------------
-------------------------------------------------------------
1_04:
-------------------------------------------------
Exceptions table: ---------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
-------------------------------------------------------------
-------------------------------------------------------------
2_01:
-------------------------------------------------
Exceptions table: ---------------------------------------------
```

```
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
------------------------------------------------------------------
------------------------------------------------------------------
2_02:
--------------------------------------------------
Exceptions table: ------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
------------------------------------------------------------------
------------------------------------------------------------------
2_03:
--------------------------------------------------
Exceptions table: ------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
------------------------------------------------------------------
------------------------------------------------------------------
2_04:
--------------------------------------------------
Exceptions table: ------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
------------------------------------------------------------------
------------------------------------------------------------------
[Expert@HostName-ch0x-0x:0]
```

asg_excp_conf del

```
[Expert@HostName-ch0x-0x:0]# asg_excp_conf del 0
1_01:
Exception ID 0 deleted
1_02:
Exception ID 0 deleted
1_03:
Exception ID 0 deleted
1_04:
Exception ID 0 deleted
2_01:
Exception ID 0 deleted
2_02:
Exception ID 0 deleted
2_03:
Exception ID 0 deleted
2_04:
Exception ID 0 deleted
[Expert@HostName-ch0x-0x:0]
```

asg_excp_conf clear

```
[Expert@HostName-ch0x-0x:0] asg_excp_conf clear
1_01:
Exception table cleared
1_02:
Exception table cleared
1_03:
Exception table cleared
1_04:
Exception table cleared
2_01:
Exception table cleared
2_02:
Exception table cleared
2_03:
Exception table cleared
2_04:
Exception table cleared
[Expert@HostName-ch0x-0x:0]
```

Installing and Uninstalling a Hotfix

This section provides instructions for installing and uninstalling a Hotfix:

- On Quantum Maestro Orchestrators

  See *"Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators" below*

- On Security Group Members

  See *"Installing and Uninstalling a Hotfix on Security Group Members" on page 354*

Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators

In This Section:

Installing a Hotfix Package on Orchestrators *351*

Uninstalling a Hotfix Package on Orchestrators *353*

Deleting a Hotfix Package on Orchestrators *353*

You use the **CPUSE** on each Quantum Maestro Orchestrator to install the applicable hotfixes.

Important:

- **It is not supported to upgrade the CPUSE Agent on Quantum Maestro Orchestrators.**
- For the **CPUSE** instructions, see sk92449.
- Jumbo Hotfix Accumulator reboots Quantum Maestro Orchestrator after installation or uninstall.
- Quantum Maestro Orchestrator stops processing traffic from the start of Jumbo Hotfix Accumulator installation or uninstall and until Quantum Maestro Orchestrator comes up from the reboot.
- You must install the same Take of Jumbo Hotfix Accumulator on all Quantum Maestro Orchestrators.

Installing a Hotfix Package on Orchestrators

Internet Connection	Installation Methods	Action Plan
Quantum Maestro Orchestrator **is** connected to the Internet	You can perform only an offline installation.	See the instructions for a Quantum Maestro Orchestrator that is **not** connected to the Internet.

Internet Connection	Installation Methods	Action Plan
Quantum Maestro Orchestrator is **not** connected to the Internet	You can perform only an offline installation.	**To install CPUSE packages in Gaia Portal** 1. Use the computer, from which you connect to Gaia Portal on Quantum Maestro Orchestrator. 2. Download the applicable CPUSE Software Packages from the *Check Point Support Center*. 3. Connect to Gaia Portal on each Quantum Maestro Orchestrator. 4. Import the applicable CPUSE Software Packages. 5. Verify the applicable CPUSE Software Packages. 6. Install the applicable CPUSE Software Packages. **To install CPUSE packages in Gaia Clish** 1. Use the computer, from which you connect to Gaia Clish on Quantum Maestro Orchestrator. 2. Download the applicable CPUSE Software Packages from the *Check Point Support Center*. 3. Transfer the applicable CPUSE Offline Software Packages to each Quantum Maestro Orchestrator to some directory (for example, `/var/log/path_to_CPUSE_packages/`). Make sure to transfer the CPUSE packages in the binary mode. 4. Connect to the command line on each Quantum Maestro Orchestrator and log in to Gaia Clish. 5. Import the applicable CPUSE Software Packages. 6. Verify the applicable CPUSE Software Packages. 7. Install the applicable CPUSE Software Packages.

Uninstalling a Hotfix Package on Orchestrators

To uninstall CPUSE packages in Gaia Portal

1. Connect to Gaia Portal on each Quantum Maestro Orchestrator.
2. Select and uninstall the applicable CPUSE Software Packages.

To uninstall CPUSE packages in Gaia Clish

1. Connect to the command line on each Quantum Maestro Orchestrator and log in to Gaia Clish.
2. Uninstall the applicable CPUSE Software Packages.

Deleting a Hotfix Package on Orchestrators

This section applies to a hotfix package that exists on the Quantum Maestro Orchestrator, but is not installed.

To delete CPUSE packages in Gaia Portal

1. Connect to Gaia Portal on each Quantum Maestro Orchestrator.
2. Select and delete the applicable CPUSE Software Packages.

To delete CPUSE packages in Gaia Clish

1. Connect to the command line on each Quantum Maestro Orchestrator and log in to Gaia Clish.
2. Delete the applicable CPUSE Software Packages.

Installing and Uninstalling a Hotfix on Security Group Members

In This Section:

Installing a Hotfix Package on Security Group Members 355
Uninstalling a Hotfix Package on Security Group Members 365

This section describes the Full Connectivity installation and uninstall of an Offline CPUSE package.

Installing a Hotfix Package on Security Group Members

Important:

- **It is not supported to upgrade the CPUSE Agent on Security Group Members.**
- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in both Security Gateway and VSX mode.
  In VSX mode, you must run all the commands in the context of VS0.
- **Do not install the hotfix on all the Security Group Members in a specific Security Group at the same time.**
- In this procedure, you divide all Security Group Members in a specific Security Group into two or more logical groups.
  In the procedure below, we use **two** logical groups denoted below as "**A**" and "**B**".
  You install the hotfix on one logical group of the Security Group Members at one time.
  The other logical group(s) of the Security Group Members continues to handle traffic.
  Each logical group should contain the same number of Security Group Members - as close as possible.

  Examples

Environment	Description
Single Site	• There are 8 Security Group Members in the Security Group. • The Logical Group "A" contains Security Group Members from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members from 1_5 to 1_8.
Single Site	• There are 5 Security Group Members in the Security Group. • The Logical Group "A" contains Security Group Members from 1_1 to 1_3. • The Logical Group "B" contains Security Group Members from 1_4 to 1_5.
Dual Site	• There are 4 Security Group Members in the Security Group (on each Site). • The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.

Installation Procedure

Step 1 - Perform the preliminary steps

For Offline CPUSE packages

Step	Instructions
A	Make sure you have the applicable CPUSE Offline package.
B	Transfer the CPUSE Offline package to the Security Group (into some directory, for example `/var/log/`).
C	Connect to the command line on the Security Group.
D	If your default shell is `/bin/bash` (the Expert mode), then go to Gaia gClish: `gclish`

E	Import the CPUSE Offline package from the hard disk:
	`installer import local /<Full Path>/<Name of the CPUSE Offline Package>`
	Example:
	`[Global] HostName-ch01-01 > installer import local /var/log/Check_Point_R80.20SP_Hotfix_Bundle_FULL.tgz`

F	Show the imported CPUSE packages: `show installer packages imported`

Step	Instructions

G	Make sure the imported CPUSE package can be installed on this Security Group:
	`installer verify [Press the Tab key]`
	`installer verify <Number of CPUSE Package>`
	Example:
	`[Global] HostName-ch01-01 > installer verify 2 member_ids all`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID  |Status  |`
	`+-----------------------------------------------------------+`
	`|1_01 (local) |Installation is allowed.  |`
	`|1_02  |Installation is allowed.  |`
	`|1_03  |Installation is allowed.  |`
	`|1_04  |Installation is allowed.  |`
	`|1_05  |Installation is allowed.  |`
	`|1_06  |Installation is allowed.  |`
	`|1_07  |Installation is allowed.  |`
	`|1_08  |Installation is allowed.  |`
	`+-----------------------------------------------------------+`
	`[Global] HostName-ch01-01 >`

Step 2 - On the Security Group, make sure to disable the SMO Image Cloning feature

Note - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is `/bin/bash` (Expert mode), then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set smo image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`

Step 3 - Install the Hotfix on the Security Group Members in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**A**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**B**" **over SSH**.
B	If your default shell is `/etc/cli.sh` (Gaia Clish), then go to the Expert mode: `expert`

C	Set the Security Group Members in the Logical Group "A" to the state "`DOWN`":
	`g_clusterXL_admin -b <SGM IDs in Group "A"> down`
	Example:
	`[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_1-1_4 down`

D	Connect to one of the Security Group Members in the Logical Group "A":
	`member <Member ID>`
	Example:
	`member 1_1`

E	Go from the Expert mode to Gaia gClish:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`gclish`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`exit`

Step	Instructions

F	Install the CPUSE hotfix package on the Security Group Members in the Logical Group "A":
	`installer install [Press the Tab key]`
	`installer install <Number of CPUSE Package> member_ids <SGM IDs in Group "A">`
	Example:
	`[Global] HostName-ch01-01 > installer install 2 member_ids 1_1-1_4`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID |Status |`
	`+-----------------------------------------------------------+`
	`|1_01 (local) |Package is ready for installation |`
	`|1_02 |Package is ready for installation |`
	`|1_03 |Package is ready for installation |`
	`|1_04 |Package is ready for installation |`
	`+-----------------------------------------------------------+`
	`The machines (1_02,1_02,1_03,1_04) will automatically reboot after install.`
	`Do you want to continue? ([y]es / [n]o) y`
	`[Global] HostName-ch01-01 >`

G	Go from Gaia gClish to the Expert mode:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`exit`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`expert`

H	Monitor the system until the Security Group Members in the Logical Group "A" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

Step 4 - Install the Hotfix on the Security Group Members in the Logical Group "B"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**B**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**A**" **over SSH**.
B	If your default shell is `/etc/cli.sh` (Gaia Clish), then go to the Expert mode: `expert`

C	Set the Security Group Members in the Logical Group "B" to the state "`DOWN`":
	`g_clusterXL_admin -b <SGM IDs in Group "B"> down`
	Example:
	`[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_5-1_8 down`

D	Connect to one of the Security Group Members in the Logical Group "B":
	`member <Member ID>`
	Example:
	`member 1_5`

E	Go from the Expert mode to Gaia gClish:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`gclish`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`exit`

Step	Instructions

F	Install the CPUSE hotfix package on the Security Group Members in the Logical Group "B":
	`installer install [Press the Tab key]`
	`installer install <Number of CPUSE Package> member_ids <SGM IDs in Group "B">`
	Example:
	`[Global] HostName-ch01-01 > installer install 2 member_ids 1_5-1_8`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID |Status |`
	`+-----------------------------------------------------------+`
	`|1_05 (local) |Package is ready for installation |`
	`|1_06 |Package is ready for installation |`
	`|1_07 |Package is ready for installation |`
	`|1_08 |Package is ready for installation |`
	`+-----------------------------------------------------------+`
	`The machines (1_05,1_06,1_07,1_08) will automatically reboot after install.`
	`Do you want to continue? ([y]es / [n]o) y`
	`[Global] HostName-ch01-01 >`

G	Go from Gaia gClish to the Expert mode:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`exit`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`expert`

H	Monitor the system until the Security Group Members in the Logical Group "B" are in the state "`UP`" and enforce the security policy again: `asg monitor`

Step 5 - Make sure the Hotfix is installed on all Security Group Members

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is `/etc/cli.sh` (Gaia Clish), then go to the Expert mode: `expert`
C	Run: `asg diag verify`

Uninstalling a Hotfix Package on Security Group Members

Important:

- **It is not supported to upgrade the CPUSE Agent on Security Group Members.**
- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in both Security Gateway and VSX mode.
  In VSX mode, you must run all the commands in the context of VS0.
- **Do not uninstall the hotfix from all the Security Group Members in a specific Security Group at the same time.**
- You uninstall the hotfix from one logical group of the Security Group Members at one time.
  The other logical group of the Security Group Members continues to handle traffic.
  You divide all Security Group Members in a specific Security Group into two logical groups - denoted below as "**A**" and "**B**".
  1. You uninstall the hotfix from the Security Group Members in the Logical Group "A"
  2. You uninstall the hotfix from the Security Group Members in the Logical Group "B"

  Each logical group should contain the same number of Security Group Members - as close as possible.

  Examples

Environment	Description
Single Site	• There are 8 Security Group Members in the Security Group. • The Logical Group "A" contains Security Group Members from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members from 1_5 to 1_8.
Single Site	• There are 5 Security Group Members in the Security Group. • The Logical Group "A" contains Security Group Members from 1_1 to 1_3. • The Logical Group "B" contains Security Group Members from 1_4 to 1_5.
Dual Site	• There are 4 Security Group Members in the Security Group (on each Site). • The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.

Uninstall Procedure

Step 1 - On the Security Group, make sure to disable the SMO Image Cloning feature

Note - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is `/bin/bash` (Expert mode), then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set smo image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`

Step 2 - Uninstall the Hotfix from the Security Group Members in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**A**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**B**" **over SSH**.
B	Go to the Expert mode.

C	Set Security Group Members in the Logical Group "A" to the state "`DOWN`":
	`g_clusterXL_admin -b <SGM IDs in Group "A"> down`
	Example:
	`[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_1-1_4 down`

D	Connect to one of the Security Group Members in the Logical Group "A": `member <Member ID>`

E	Go from the Expert mode to Gaia gClish:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`gclish`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`exit`

Step	Instructions

F	Uninstall the CPUSE hotfix package on the Security Group Members in the Logical Group "A":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids <SGM IDs in Group "A">`
	Example:
	`[Global] HostName-ch01-01 > installer uninstall 2 member_ids 1_1-1_4`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID  |Status                                       |`
	`+-------------+-------------------------------------------+`
	`|1_01 (local) |Package is ready for uninstallation        |`
	`|1_02        |Package is ready for uninstallation        |`
	`|1_03        |Package is ready for uninstallation        |`
	`|1_04        |Package is ready for uninstallation        |`
	`+-------------+-------------------------------------------+`
	`The machines (1_02,1_02,1_03,1_04) will automatically reboot after uninstall.`
	`Do you want to continue? ([y]es / [n]o) y`
	`[Global] HostName-ch01-01 >`

G	Go from Gaia gClish to the Expert mode:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`exit`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`expert`

H	Monitor the system until the Security Group Members in the Logical Group "A" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

Step 3 - Uninstall the Hotfix from the Security Group Members in the Logical Group "B"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**B**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**A**" **over SSH**.
B	Go to the Expert mode: `expert`

C	Set Security Group Members in the Logical Group "B" to the state "`DOWN`":
	`g_clusterXL_admin -b <SGM IDs in Group "B"> down`
	Example:
	`[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_5-1_8 down`

D	Connect to one of the Security Group Members in the Logical Group "A": `member <Member ID>`

E	Go from the Expert mode to Gaia gClish:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`gclish`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`exit`

Step	Instructions

F	Uninstall the CPUSE hotfix package on the Security Group Members in the Logical Group "B":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids <SGM IDs in Group "B">`
	Example:
	`[Global] HostName-ch01-01 > installer uninstall 2 member_ids 1_5-1_8`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID |Status |`
	`+-----------------------------------------------------------+`
	`|1_05 (local) |Package is ready for uninstallation |`
	`|1_06 |Package is ready for uninstallation |`
	`|1_07 |Package is ready for uninstallation |`
	`|1_08 |Package is ready for uninstallation |`
	`+-----------------------------------------------------------+`
	`The machines (1_05,1_06,1_07,1_08) will automatically reboot after uninstall.`
	`Do you want to continue? ([y]es / [n]o) y`
	`[Global] HostName-ch01-01 >`

G	Go from Gaia gClish to the Expert mode:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`exit`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`expert`

H	Monitor the system until the Security Group Members in the Logical Group "A" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

Step 4 - Make sure the Hotfix is uninstalled from all Security Group Members

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is `/etc/cli.sh` (Gaia Clish), then go to the Expert mode: `expert`
C	Run: `asg diag verify`

Configuring Security Group High Availability

In This Section:

Setting Security Group Weights (High Availability Factors) 372
Setting the Quality Grade Differential 373

Setting Security Group Weights (High Availability Factors)

Each hardware component in a Security Group Member has a quality weight factor, which sets its relative importance to overall Security Group health.

For example, ports are more important than other components and are typically assigned a higher weight value.

The Security Group Member grade is the sum of all component weight values.

In a dual Dual Site environment, the Security Group with the higher grade becomes Active and handles traffic.

The grade for each component is calculated based on this formula:

```
(Unit Weight) x (Number of components in the UP state)
```

To see the weight of each component, run in Gaia gClish on a Security Group:

```
asg stat -v
```

Description

Use the "`set chassis high-availability factors`" command to configure a hardware component's weight.

Syntax in Gaia gClish of the Security Group

```
set chassis high-availability factors sgm <SGM Factor>
```

```
set chassis high-availability factors port {other <Other Port Factor> | standard <Standard Port Factor> | mgmt <Management Port Factor> | bond <Bond Port Factor>}
```

Parameters

Parameter	Description
<SGM Factor>	Weight factor for a Security Group Member. Valid range: integer between 0 and 1000.
<Other Port Factor>	High grade port factor. Valid range: integer between 0 and 1000.
<Standard Port Factor>	Standard grade port factor. Valid range: integer between 0 and 1000.
<Management Port Factor>	Management port factor. Valid range: integer between 0 and 1000.
<Bond Port Factor>	Bond interface factor. Valid range: integer between 0 and 1000.

Examples

```
[Global] MyChassis-ch01-01 > set chassis high-availability factors sgm 100
[Global] MyChassis-ch01-01 > set chassis high-availability factors port other 70
[Global] MyChassis-ch01-01 > set chassis high-availability factors port standard 50
```

Setting the Quality Grade Differential

Description

Use the "`set chassis high-availability failover`" command in Gaia gClish to set the minimum quality grade differential that causes a failover.

Syntax in Gaia gClish of the Security Group

```
set chassis high-availability failover <Trigger>
```

Parameters

Parameter	Description
<Trigger>	Minimum difference in Chassis quality grade to trigger a failover. Valid values: 1 - 1000.

IP Block and URL Block Features

Starting in Take 210 of R80.20SP Jumbo Hotfix Accumulator (sk155832), you can use new tools to block malicious traffic:

The "`ip_block`" command that lets you block malicious traffic to or from certain IP addresses (see *"IP Block Feature" below*).

The "`url_block`" command that lets you block malicious traffic to or from certain URLs (see *"URL Block Feature" on page 379*).

In addition, refer to sk103154.

IP Block Feature

In This Section:

Description *374*

CLI *375*

Procedure *376*

Description

The IP Block feature provides the ability to block malicious traffic to and from certain IP addresses.

The IP Block feature requires the list of malicious IP addresses as a feed (URL).

The IP Block feature runs periodically, fetches the IP list again and updates the IP addresses in the Security Gateway based on the list in the feed.

The blocking mechanism is enforced by an Access Control rule with a Dynamic Object.

Check Point's Security Intelligence maintains and periodically updates a list of IP addresses known as TOR Exit Nodes:

```
https://secureupdates.checkpoint.com/IP-list/TOR.txt
```

Best Practice - We recommend to consider the "Custom Intelligence Feeds" from sk132193.

Notes:

- These IP ranges are excluded by default: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.
- The IP Block feature supports only IPv4 feeds.

CLI

Syntax

`ip_block -h`
`ip_block -s SET_DYN_OBJ`
`ip_block -n`
`ip_block -a ADD_URL [ADD_URL ...]`
`ip_block -d DEL_URL`
`ip_block -l [-j]`
`ip_block -e ACTIVATE`
`ip_block -x`
`ip_block -c`
`ip_block -r [-f]`

Parameters

Parameter	Description
`-h` `--help`	Shows the built-in help.
`-a ADD_URL [ADD_URL ...]` `--add-url ADD_URL [ADD_URL ...]`	Adds IP feed URLs (separated by a comma) to the configuration.
`-d DEL_URL` `--del-url DEL_URL`	Deletes IP feed URLs (separated by a comma) from the configuration.
`-l` `--list-urls`	Shows the configured IP feed URLs.
`-s SET_DYN_OBJ` `--set-dynamic-object SET_DYN_OBJ`	Specifies the Dynamic Object name in the configuration. For example, `MyDynObj`.
`-n` `--show-dynamic-object-name`	Show the configured Dynamic Object name.

Parameter	Description
`-r` `--run`	Updates the IP addresses in the configuration.
`-f` `--force`	Forces the update.
`-j` `--json`	Shows the output in JSON format.
`-c` `--clear-cache`	Clears the cache.
`-e` *`ACTIVATE`* `--activate` *`ACTIVATE`*	Starts the periodic run of the feature at the specified intervals. Specify the interval ACTIVATE as a number followed by units: ■ `Xs` - runs every X seconds (for example, 30s) ■ `Xm` - runs every X minutes (for example, 20m) ■ `Xh` - runs every X hours (for example, 1h)
`-x` `--deactivate`	Stops the periodic run of the feature.

Procedure

Follow these steps in SmartConsole and on the Security Group.

Procedure

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	Create a new Dynamic Object: From the right panel **Objects**, click **New > More > Network Object > Dynamic Objects > Dynamic Object**.
3	In the **New Dynamic Object** window, enter a name (for example, `MyDynObj`) and click **OK**. You use this name later in the CLI on the Security Group.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>4</td><td>In the applicable Access Control policy, add a new rule that drops all traffic from the new Dynamic Object:
<table>
<tr><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th><th>Track</th></tr>
<tr><td>Dynamic Object</td><td>Any</td><td>Any</td><td>Any</td><td>Drop</td><td>None</td></tr>
</table></td></tr>
<tr><td>5</td><td>Connect to the command line on the Security Group.</td></tr>
<tr><td>6</td><td>Log in to the Expert mode.</td></tr>
<tr><td>7</td><td>Configure the Dynamic Object as configured in SmartConsole:
<code>dynamic_objects -n <Name of Dynamic Object in SmartConsole></code></td></tr>
<tr><td>8</td><td>Examine the Dynamic Objects configuration to make sure the new Dynamic Object is added:
<code>dynamic_objects -l</code></td></tr>
<tr><td>9</td><td>Configure the Dynamic Object in the IP Block settings as configured in SmartConsole:
<code>ip_block --set-dynamic-object <<i>Name of Dynamic Object in SmartConsole</i>></code></td></tr>
<tr><td>10</td><td>Examine the IP Block configuration to make sure the new Dynamic Object is added:
<code>ip_block --show-dynamic-object-name</code></td></tr>
<tr><td>11</td><td>Configure the URL for the IP feed:
<code>ip_block --add-url <URL></code>
Example:
<code>ip_block --add-url
https://secureupdates.checkpoint.com/IP-list/TOR.txt</code>
Note - This can be a file on your own web server.</td></tr>
<tr><td>12</td><td>Examine the configuration to make sure the feed URL is added:
<code>ip_block --list-urls</code></td></tr>
</table>

Step	Instructions
13	Start the periodic run at the specified intervals: `ip_block --activate <ACTIVATE>`

14	Examine the configuration to make sure the "ip_block" command is scheduled to run at the specified intervals by the CPD daemon:
	`cpd_sched_config print | grep -A 5 "ip_block"`
	Example output:
	`Task: "ip_block"`
	`Command: /bin/ip_block`
	`Arguments: -r`
	`Interval: 600`
	`Active: true`
	`RunAtStart: false`

15	In SmartConsole, install the Access Control Policy on the Security Group object.
16	Examine the log on the Security Group: `/var/log/ip_block.elg`

URL Block Feature

In This Section:

Description 379
CLI 379
Procedure 380

Description

The URL Block feature provides the ability to block malicious traffic to and from certain URLs.

The URL Block feature requires the list of malicious URLs as a feed (URL).

The URL Block feature runs periodically, fetches the URL list again and updates the URLs in the Security Gateway based on the list in the feed.

The blocking mechanism is enforced by an Access Control rule with a custom Application.

CLI

Syntax

```
url_block -h
```

```
url_block -a -n <NAME> -p <URL> -z {true | false} [-x
<PASSWORD>] -r {true | false}
```

```
url_block -d -n <NAME>
```

```
url_block -i <INTERVAL>
```

```
url_block -l
```

Parameters

Parameter	Description
`-h` `--help`	Shows the built-in help.
`-a` `--add-url`	Adds URL feed to the configuration.
`-n <NAME>`	Specifies the name of the custom Application object as configured in SmartConsole.

Parameter	Description
`-p <URL>` `--path <URL>`	Specifies the URL of your web server that hosts the file with the list of malicious URLs. Example: `http://192.168.20.30/` **Note** - This URL must end with the slash and must not contain the name of the file.
`-d` `--del-url`	Deletes URL feed from the configuration.
`-z {true | false}` `--zip {true | false}`	Specifies that URL feed is a ZIP archive (value "true").
`-x <PASSWORD>` `--zip-pass <PASSWORD>`	Specifies the password for the ZIP archive with the URL feed.
`-r {true | false}` `--regex {true | false}`	You must specify this parameter with the value "true", if in SmartConsole in the object of the custom Application you selected **URLs are defined as Regular Expressions**. Otherwise, you must specify this parameter with the value "false".
`-l` `--list-urls`	Shows the configured URL feed.
`-i <INTERVAL>` `--interval <INTERVAL>`	Specifies the interval in seconds.

Procedure

Follow these steps in SmartConsole and on the Security Group.

Procedure

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>1</td><td>Prepare a plain text file with the list of malicious URLs:
a. Each URL must be on a separate line.
b. The name of this file must be urls.txt (case sensitive).
c. Place this file on your web server.</td></tr>
<tr><td>2</td><td>Connect with SmartConsole to the Management Server.</td></tr>
<tr><td>3</td><td>Create a new custom Application object:
From the right panel Objects, click New > More > Custom Application/Site > Application/Site.</td></tr>
<tr><td>4</td><td>In the Application/Site window:
a. Enter a name (for example, MyURLs)
You use this name later in the CLI on the Scalable Platform.
b. From the left, click the General page.
c. In the General section, in the Primary Category field, select Custom_Application_Site.
d. In the Match By section, click the plus icon (+) and add the URL of the web server that hosts the file with the list of malicious URLs.
Example: <code>http://192.168.20.30/</code>
Note - This URL must end with the slash and must not contain the name of the file (urls.txt).
e. Click OK.</td></tr>
<tr><td>5</td><td>In the applicable Access Control policy, add a new rule that drops all traffic that matches the new Application:
<table>
<tr><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th><th>Track</th></tr>
<tr><td>Any</td><td>Any</td><td>Any</td><td>Object of the Custom Application</td><td>Drop</td><td>None</td></tr>
</table></td></tr>
<tr><td>6</td><td>Connect to the command line on the Security Group.</td></tr>
<tr><td>7</td><td>Log in to the Expert mode.</td></tr>
</table>

Step	Instructions

8	Configure the URL for the feed:
	`url_block -a -n <Name of Custom Application Object> -p <URL of Your Web Server> ...`
	Example:
	`url_block -a -n MyUrls -p http://192.168.20.30/ -z false -r false`
	Note - This can be a file on your own web server.

9	Start the periodic run at the specified intervals: `url_block -i <INTERVAL>`

10	Examine the configuration:
	`url_block -l`
	Example output:
	`Refresh time interval: 300`
	`MyUrls`
	`Path: http://192.168.20.30/`
	`Zip: false`
	`Regex: false`

11	In SmartConsole, install the Access Control Policy on the Security Group object.
12	Examine the log on the Security Group: `/var/log/rul_block.elg`

Deploying a Security Group in Monitor Mode

In This Section:

Introduction to Monitor Mode 383
Example Topology for Monitor Mode 384
Supported Software Blades in Monitor Mode 385
Limitations in Monitor Mode 387

Introduction to Monitor Mode

You can configure Monitor Mode on one Security Group's interface.

The Security Group listens to traffic from a Mirror Port (or Span Port) on a connected switch.

Use the Monitor Mode to analyze network traffic without changing the production environment.

The mirror port on a switch duplicates the network traffic and sends it to the Security Group with an interface configured in Monitor Mode to record the activity logs.

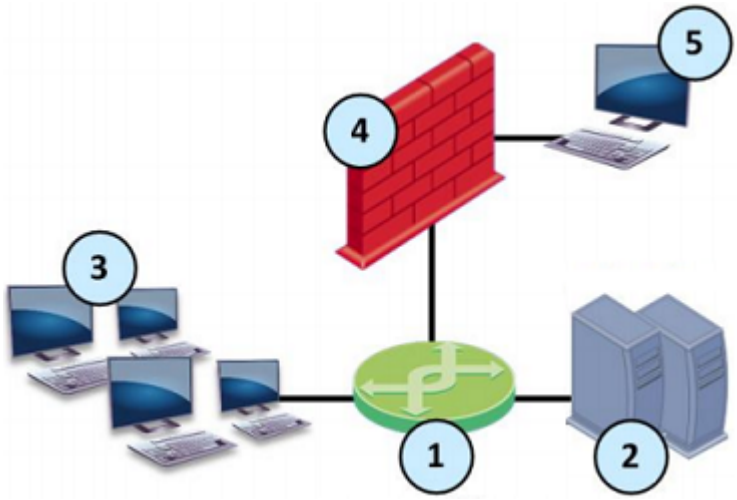
You can use the Monitor Mode:

- To monitor the use of applications as a permanent part of your deployment
- To evaluate the capabilities of the Software Blades:
  - The Security Group neither enforces any security policy, nor performs any active operations (prevent / drop / reject) on the interface in the Monitor Mode.
  - The Security Group terminates and does not forward all packets that arrive at the interface in the Monitor Mode.
  - The Security Group does not send any traffic through the interface in the Monitor Mode.

Benefits of the Monitor Mode include:

- There is no risk to your production environment.
- It requires minimal set-up configuration.
- It does not require TAP equipment, which is expensive.

Example Topology for Monitor Mode



Item	Description
1	Switch with a mirror or SPAN port that duplicates all incoming and outgoing packets. The Security Group connects to a mirror or SPAN port on the switch.
2	Servers.
3	Clients.
4	Security Group with an interface in Monitor Mode.
5	Security Management Server that manages the Security Group.

Supported Software Blades in Monitor Mode

This table lists Software Blades and their support for the Monitor Mode.

Software Blade	Support for the Monitor Mode
Firewall	Fully supports the Monitor Mode.
IPS	These protections and features do **not** work: ■ The **SYN Attack** protection (SYNDefender). ■ The **Initial Sequence Number (ISN) Spoofing** protection. ■ The **Send error page** action in Web Intelligence protections. ■ Client and Server notifications about connection termination.
Application Control	Does **not** support UserCheck.
URL Filtering	Does **not** support UserCheck.
Data Loss Prevention	Does **not** support these: ■ UserCheck. ■ The "**Prevent**" and "**Ask User**" actions - these are automatically demoted to the "**Inform User**" action. ■ FTP inspection.
Identity Awareness	Does **not** support these: ■ Captive Portal. ■ Identity Agent.
Threat Emulation	Does **not** support these: ■ The Emulation Connection Prevent Handling Modes "**Background**" and "**Hold**". See sk106119. ■ FTP inspection.
Content Awareness	Does **not** support the FTP inspection.
Anti-Bot	Fully supports the Monitor Mode.
Anti-Virus	Does **not** support the FTP inspection.
IPsec VPN	Does **not** support the Monitor Mode.
Mobile Access	Does **not** support the Monitor Mode.

Software Blade	Support for the Monitor Mode
Anti-Spam & Email Security	Does **not** support the Monitor Mode.
QoS	Does **not** support the Monitor Mode.

Limitations in Monitor Mode

These features and deployments are **not** supported in Monitor Mode:

- Passing production traffic through a Security Gateway, on which you configured Monitor Mode interface(s).
- If you configure more than one Monitor Mode interface on a Security Gateway, you must make sure the Security Gateway does not receive the same traffic on the different Monitor Mode interfaces.
- HTTPS Inspection
- NAT rules.
- HTTP / HTTPS proxy.
- Anti-Virus in Traditional Mode.
- User Authentication.
- Client Authentication.
- Check Point Active Streaming (CPAS).
- Cluster deployment.
- CloudGuard Gateways.
- CoreXL Dynamic Dispatcher (sk105261).
- Setting the value of the kernel parameters "`psl_tap_enable`" and "`fw_tap_enable`" to 1 (one) on-the-fly with the "`fw ctl set int`" command (Issue ID 02386641).

For more information, see sk101670: Monitor Mode on Gaia OS and SecurePlatform OS.

Configuring a Security Group in Gateway mode in Monitor Mode

Important:

- For Cloud-based services (for example, Social Network widgets and URL Filtering), you must connect the Security Group in Monitor Mode to the Internet.
- You must install valid license and contracts file on the Security Group in Monitor Mode.

Procedure:

1. **Install the environment**

   For more information, see the *Quantum Maestro Getting Started Guide*.

Step	Instructions
1	Install the Maestro environment.
2	Configure the applicable Security Group and assign the applicable interface(s).
3	Run the Gaia First Time Configuration Wizard for the Security Group.
4	During the First Time Configuration Wizard, you must configure these settings: ■ In the **Management Connection** window, select the interface, through which you connect to Gaia operating system. ■ In the **Internet Connection** window, do not configure IP addresses. ■ In the **Installation Type** window, select **Security Gateway and/or Security Management**. ■ In the **Products** window: a. In the **Products** section, select **Security Gateway** only. b. In the **Clustering** section, clear **Unit is a part of a cluster, type**. ■ In the **Dynamically Assigned IP** window, select **No**. ■ In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

2. **Configure the Monitor Mode on the applicable interface**

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia gClish of the Security Group.

Configuring the Monitor Mode in Gaia Portal

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	In the left navigation tree, click **Network Management** > **Network Interfaces**.
3	Select the applicable physical interface from the list and click **Edit**.
4	Select the **Enable** option to set the interface status to UP.
5	In the **Comment** field, enter the applicable comment text (up to 100 characters).
6	On the **IPv4** tab, select **Use the following IPv4 address**, but do **not** enter an IPv4 address.
7	On the **IPv6** tab, select **Use the following IPv6 address**, but do **not** enter an IPv6 address. **Important** - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the **Ethernet** tab: ■ Select **Auto Negotiation**, or select a link speed and duplex setting from the list. ■ In the **Hardware Address** field, enter the Hardware MAC address (if not automatically received from the NIC). **Caution** - Do **not** manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure. ■ In the **MTU** field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500). ■ Select **Monitor Mode**.
9	Click **OK**.

Configuring the Monitor Mode in Gaia gClish

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to Gaia Clish.
3	Go to Gaia gClish: enter `gclish` and press Enter.
4	Examine the configuration and state of the applicable physical interface: `show interface <Name of Physical Interface>`

5	If the applicable physical interface has an IP address assigned to it, remove that IP address.
	■ To remove an IPv4 address:
	`delete interface <Name of Physical Interface> ipv4-address`
	■ To remove an IPv6 address:
	`delete interface <Name of Physical Interface> ipv6-address`

6	Enable the Monitor Mode on the physical interface: `set interface <Name of Physical Interface> monitor-mode on`
7	Configure other applicable settings on the interface in the Monitor Mode: `set interface <Name of Physical Interface> ...`
8	Examine the configuration and state of the Monitor Mode interface: `show interface <Name of Physical Interface>`
9	Save the configuration: `save config`

3. **Configure the Security Gateway object in SmartConsole**

   You can configure the applicable Security Gateway object in SmartConsole either in Wizard Mode, or in Classic Mode.

Configuring the Security Gateway object in Wizard Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**.
4	In the **Check Point Security Gateway Creation** window, click **Wizard Mode**.
5	On the **General Properties** page: a. In the **Gateway name** field, enter the applicable name for this Security Gateway object. b. In the **Gateway platform** field, select Maestro. c. In the **Gateway IP address** section, select **Static IP address** and configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses. d. Click **Next**.
6	On the **Trusted Communication** page: a. Select the applicable option: ■ If you selected **Initiate trusted communication now**, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. ■ If you selected **Skip and initiate trusted communication later**, make sure to follow **Step 7**. b. Click **Next**.

Step	Instructions
7	On the **End** page: a. Examine the **Configuration Summary**. b. Select **Edit Gateway properties for further configuration**. c. Click **Finish**. **Check Point Gateway** properties window opens on the **General Properties** page.
8	If during the Wizard Mode, you selected **Skip and initiate trusted communication later**: a. The **Secure Internal Communication** field shows **Uninitialized**. b. Click **Communication**. c. In the **Platform** field select Maestro. d. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. e. Click **Initialize**. Make sure the **Certificate state** field shows **Established**. f. Click **OK**.
9	On the **Network Security** tab, make sure to enable only the Firewall Software Blade.
10	On the **Network Management** page: a. Click **Get Interfaces** > **Get Interfaces with Topology**. b. Confirm the interfaces information.
11	Select the interface in the Monitor Mode and click **Edit**. Configure these settings: a. Click the **General** page. b. In the **General** section, enter a *random* IPv4 address. **Important** - This random IPv4 address must not conflict with existing IPv4 addresses on your network. c. In the **Topology** section: Click **Modify**. In the **Leads To** section, select **Not defined (Internal)**. In the **Security Zone** section, select **According to topology: Internal Zone**. Click **OK** to close the **Topology Settings** window. d. Click **OK** to close the **Interface** window.
12	Click **OK**.

Step	Instructions
13	Publish the SmartConsole session.
14	This Security Gateway object is now ready to receive the Security Policy.

Configuring the Security Gateway in Classic Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**.
4	In the **Check Point Security Gateway Creation** window, click **Classic Mode**. **Check Point Gateway** properties window opens on the **General Properties** page.
5	In the **Name** field, enter the applicable name for this Security Gateway object.
6	In the **IPv4 address** and **IPv6 address** fields, configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.

Step	Instructions
7	Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group: a. Near the **Secure Internal Communication** field, click **Communication**. b. In the **Platform** field select Maestro. c. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. d. Click **Initialize**. e. Click **OK**.

	If the **Certificate state** field does not show `Established`, perform these steps:
	a. Connect to the command line on the Security Group.
	b. Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).
	c. Run:
	`cpconfig`
	d. Enter the number of this option:
	`Secure Internal Communication`
	e. Follow the instructions on the screen to change the Activation Key.
	f. In SmartConsole, click **Reset**.
	g. Enter the same Activation Key you entered in the `cpconfig` menu.
	h. In SmartConsole, click **Initialize**.

8	In the **Platform** section, select the correct options: a. In the **Hardware** field, select Maestro. b. In the **Version** field, select **R80.20SP**. c. In the **OS** field, select **Gaia**.
9	On the **Network Security** tab, make sure to enable only the Firewall Software Blade. **Important** - Do **not** select anything on the **Management** tab.

Step	Instructions
10	On the **Network Management** page: a. Click **Get Interfaces** > **Get Interfaces with Topology**. b. Confirm the interfaces information.
11	Select the interface in the Monitor Mode and click **Edit**. Configure these settings: a. Click the **General** page. b. In the **General** section, enter a *random* IPv4 address. **Important** - This random IPv4 address must not conflict with existing IPv4 addresses on your network. c. In the **Topology** section: Click **Modify**. In the **Leads To** section, select **Not defined (Internal)**. In the **Security Zone** section, select **According to topology: Internal Zone**. Click **OK** to close the **Topology Settings** window. d. Click **OK** to close the **Interface** window.
12	Click **OK**.
13	Publish the SmartConsole session.
14	This Security Gateway object is now ready to receive the Security Policy.

4. **Configure the Security Group to process packets that arrive in the wrong order**

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Set the value of the kernel parameter **psl_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Passive Streaming Layer (PSL) Tap Mode:: `g_update_conf_file fwkern.conf psl_tap_enable=1`

Step	Instructions
4	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file fwkern.conf fw_tap_enable=1`
5	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$PPKDIR/conf/simkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file $PPKDIR/conf/simkern.conf fw_tap_enable=1`
6	Reboot the Security Group.
7	Connect to the command line on the Security Group.
8	Log in to the Expert mode.

9	Make sure the Security Group loaded the new configuration:
	`g_fw ctl get int psl_tap_enable`
	`g_fw ctl get int fw_tap_enable`

Notes:

- This configuration helps the Security Group process packets that arrive in the wrong or abnormal order (for example, TCP [SYN-ACK] arrives before TCP [SYN]).
- This configuration helps the Security Group work better for the first 10-30 minutes when it processes connections, in which the TCP [SYN] packets did not arrive.
- This configuration is also required when you use a TAP device or Mirror / Span ports with separated TX/RX queues.
- This configuration will make the Mirror Port on Security Group work better for the first 10-30 minutes when processing connections, in which the TCP-SYN packet did not arrive.
- It is not possible to set the value of the kernel parameters "`psl_tap_enable`" and "`fw_tap_enable`" on-the-fly with the "`g_fw ctl set int <parameter>`" command (Known Limitation 02386641).

5. **Configure the required Global Properties for the Security Group in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Target* Domain Management Server that manages this Security Group.
2	In the top left corner, click **Menu > Global properties**.
3	From the left tree, click the **Stateful Inspection** pane and configure: a. In the **Default Session Timeouts** section: i. Change the value of the **TCP session timeout** from the default **3600** to **60** seconds. ii. Change the value of the **TCP end timeout** from the default **20** to **5** seconds. b. In the **Out of state packets** section, you must clear all the boxes. Otherwise, the Security Group drops the traffic as out of state (because the traffic does not pass through the Security Group, it does not record the state information for the traffic).
4	From the left tree, click the **Advanced** page > click the **Configure** button, and configure: a. Click **FireWall-1** > **Stateful Inspection**. b. Clear **reject_x11_in_any**. c. Click **OK** to close the **Advanced Configuration** window.
5	Click **OK** to close the **Global Properties** window.
6	Publish the SmartConsole session.

6. **Configure the required Access Control Policy for the Security Group in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click **Security Policies**.
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>4</td><td>Create the Access Control rule that accepts all traffic:
<table>
<tr><th>No</th><th>Name</th><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th><th>Track</th><th>Install On</th></tr>
<tr><td>1</td><td>Accept All</td><td>*Any</td><td>*Any</td><td>Any</td><td>*Any</td><td>Accept</td><td>Log</td><td>Object of Security Gateway in Monitor Mode</td></tr>
</table></td></tr>
<tr><td>5</td><td>Best Practice
We recommend these Aggressive Aging settings for the most common TCP connections:
a. In the SmartConsole, click Objects menu > Object Explorer.
b. Open Services and select TCP.
c. Search for the most common TCP connections in this network.
d. Double-click the applicable TCP service.
e. From the left tree, click Advanced.
f. At the top, select Override default settings.
On Domain Management Server, select Override global domain settings.
g. Select Match for 'Any'.
h. In the Aggressive aging section:
Select Enable aggressive aging.
Select Specific and enter 60.
i. Click OK.
j. Close the Object Explorer.</td></tr>
<tr><td>6</td><td>Publish the SmartConsole session.</td></tr>
<tr><td>7</td><td>Install the Access Control Policy on the Security Gateway object.</td></tr>
</table>

7. **Make sure the Security Group enabled the Monitor Mode for Software Blades**

Step	Instructions
1	Connect to the command line on the Security Group.

Step	Instructions
2	Log in to the Expert mode.

3	Install the default policy on the VSX Gateway object:
	Make sure the parameter **fw_span_port_mode** is part of the installed policy:
	`grep -A 3 -r fw_span_port_mode $FWDIR/state/local/*`
	The returned output must show:
	`:val (true)`

8. **Connect the Security Group to the switch**

   Connect the interface in the Monitor Mode to the mirror or SPAN port on the switch.

For more information, see the:

- *Quantum Maestro Getting Started Guide*.
- *R80.20SP Quantum Maestro Gaia Administration Guide*.
- *R80.20 Security Management Administration Guide*.

Configuring a Security Group in VSX mode in Monitor Mode

Important:

- For Cloud-based services (for example, Social Network widgets and URL Filtering), you must connect the Security Group in Monitor Mode to the Internet (also, see sk79700 and sk106496).
- You must install valid license and contracts file on the Security Group in Monitor Mode.

Procedure:

1. **Install the environment**

   For more information, see the *Quantum Maestro Getting Started Guide*.

Step	Instructions
1	Install the Maestro environment.
2	Configure the applicable Security Group.
3	Run the Gaia First Time Configuration Wizard for the Security Group.
4	During the First Time Configuration Wizard, you must configure these settings: ■ In the **Management Connection** window, select the interface, through which you connect to Gaia operating system. ■ In the **Internet Connection** window, do not configure IP addresses. ■ In the **Installation Type** window, select **Security Gateway and/or Security Management**. ■ In the **Products** window: a. In the **Products** section, select **Security Gateway** only. b. In the **Clustering** section, clear **Unit is a part of a cluster, type**. ■ In the **Dynamically Assigned IP** window, select **No**. ■ In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

2. **Configure the Monitor Mode on the applicable interface**

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia gClish of the Security Group.

Configuring the Monitor Mode in Gaia Portal

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	In the left navigation tree, click **Network Management** > **Network Interfaces**.
3	Select the applicable physical interface from the list and click **Edit**.
4	Select the **Enable** option to set the interface status to UP.
5	In the **Comment** field, enter the applicable comment text (up to 100 characters).
6	On the **IPv4** tab, select **Use the following IPv4 address**, but do **not** enter an IPv4 address.
7	On the **IPv6** tab, select **Use the following IPv6 address**, but do **not** enter an IPv6 address. **Important** - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the **Ethernet** tab: ■ Select **Auto Negotiation**, or select a link speed and duplex setting from the list. ■ In the **Hardware Address** field, enter the Hardware MAC address (if not automatically received from the NIC). **Caution** - Do **not** manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure. ■ In the **MTU** field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500). ■ Select **Monitor Mode**.
9	Click **OK**.

Configuring the Monitor Mode in Gaia gClish

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to Gaia Clish.
3	Go to Gaia gClish: enter `gclish` and press Enter.
4	Examine the configuration and state of the applicable physical interface: `show interface <Name of Physical Interface>`

5	If the applicable physical interface has an IP address assigned to it, remove that IP address.
	■ To remove an IPv4 address:
	`delete interface <Name of Physical Interface> ipv4-address`
	■ To remove an IPv6 address:
	`delete interface <Name of Physical Interface> ipv6-address`

6	Enable the Monitor Mode on the physical interface: `set interface <Name of Physical Interface> monitor-mode on`
7	Configure other applicable settings on the interface in the Monitor Mode: `set interface <Name of Physical Interface> ...`
8	Examine the configuration and state of the Monitor Mode interface: `show interface <Name of Physical Interface>`
9	Save the configuration: `save config`

3. **Configure the Security Group to process packets that arrive in the wrong order**

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Set the value of the kernel parameter **psl_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Passive Streaming Layer (PSL) Tap Mode:: `g_update_conf_file fwkern.conf psl_tap_enable=1`
4	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file fwkern.conf fw_tap_enable=1`
5	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$PPKDIR/conf/simkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file $PPKDIR/conf/simkern.conf fw_tap_enable=1`
6	Reboot the Security Group.
7	Connect to the command line on the Security Group.
8	Log in to the Expert mode.

9	Make sure the Security Group loaded the new configuration:
	`g_fw ctl get int psl_tap_enable`
	`g_fw ctl get int fw_tap_enable`

Notes:

- This configuration helps the Security Group process packets that arrive in the wrong or abnormal order (for example, TCP [SYN-ACK] arrives before TCP [SYN]).
- This configuration helps the Security Group work better for the first 10-30 minutes when it processes connections, in which the TCP [SYN] packets did not arrive.
- This configuration is also required when you use a TAP device or Mirror / Span ports with separated TX/RX queues.
- This configuration will make the Mirror Port on Security Group work better for the first 10-30 minutes when processing connections, in which the TCP-SYN packet did not arrive.
- It is not possible to set the value of the kernel parameters "`psl_tap_enable`" and "`fw_tap_enable`" on-the-fly with the "`g_fw ctl set int <parameter>`" command (Known Limitation 02386641).

4. **Configure the VSX Gateway object in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Main* Domain Management Server that should manage this VSX Gateway.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new VSX Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✶) > **VSX** > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **VSX** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **VSX** > **Gateway** The **VSX Gateway Wizard** opens.
4	On the **VSX Gateway General Properties (Specify the object's basic settings)** page: a. In the **Enter the VSX Gateway Name** field, enter the applicable name for this VSX Gateway object. b. In the **Enter the VSX Gateway IPv4** field, enter the same IPv4 address that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. c. In the **Enter the VSX Gateway IPv6** field, enter the same IPv6 address that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. d. In the **Select the VSX Gateway Version** field, select **R80.20SP**. e. Click **Next**.

Step	Instructions
5	On the **VSX Gateway General Properties (Secure Internal Communication)** page: a. In the **Activation Key** field, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. b. In the **Confirm Activation Key** field, enter the same Activation Key again. c. Click **Initialize**. d. Click **Next**.

	If the **Trust State** field does not show **Trust established**, perform these steps:
	a. Connect to the command line on the Security Group.
	b. Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).
	c. Run:
	`cpconfig`
	d. Enter the number of this option:
	`Secure Internal Communication`
	e. Follow the instructions on the screen to change the Activation Key.
	f. In SmartConsole, on the **VSX Gateway General Properties** page, click **Reset**.
	g. Enter the same Activation Key you entered in the `cpconfig` menu.
	h. In SmartConsole, click **Initialize**.

6	On the **VSX Gateway Interfaces (Physical Interfaces Usage)** page: a. Examine the list of the interfaces - it must show all the physical interfaces on the Security Group. b. If you plan to connect more than one Virtual System directly to the same physical interface, you must select **VLAN Trunk** for that physical interface. c. Click **Next**.
7	On the **Virtual Network Device Configuration (Specify the object's basic settings)** page: a. You can select **Create a Virtual Network Device** and configure the first applicable Virtual Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router. b. Click **Next**.

Step	Instructions
8	On the **VSX Gateway Management (Specify the management access rules)** page: a. Examine the default access rules. b. Select the applicable default access rules. c. Configure the applicable source objects, if needed. d. Click **Next**. **Important** - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.
9	On the **VSX Gateway Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.
10	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`
11	Install the default policy on the VSX Gateway object: a. Click **Install Policy**. b. In the **Policy** field, select the default policy for this VSX Gateway object. This policy is called: `<Name of VSX Gateway object>_VSX` c. Click **Install**.
12	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

5. **Configure the Virtual System object (and other Virtual Devices) in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server, or each *Target* Domain Management Server that should manage each Virtual Device.
2	Configure the applicable Virtual System (and other Virtual Devices) on this VSX Gateway. When you configure this Virtual System, for the Monitor Mode interface, add a regular interface. In the **IPv4 Configuration** section, enter a *random* IPv4 address. **Important** - This random IPv4 address must not conflict with existing IPv4 addresses on your network.
3	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`
4	Disable the Anti-Spoofing on the interface that is configured in the Monitor Mode: a. In SmartConsole, open the Virtual System object. b. Click the **Topology** page. c. Select the Monitor Mode interface and click **Edit**. The **Interface Properties** window opens. d. Click the **General** tab. e. In the **Security Zone** field, select **None**. f. Click the **Topology** tab. g. In the **Topology** section, make sure the settings are **Internal (leads to the local network)** and **Not Defined**. h. In the **Anti-Spoofing** section, clear **Perform Anti-Spoofing based on interface topology**. i. Click **OK** to close the **Interface Properties** window. j. Click **OK** to close the **Virtual System Properties** window. k. The Management Server pushes the VSX Configuration.

6. **Configure the required Global Properties for the Virtual System in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Target*Domain Management Server that manages this Virtual System.

Step	Instructions
2	In the top left corner, click **Menu > Global properties**.
3	From the left tree, click the **Stateful Inspection** pane and configure: a. In the **Default Session Timeouts** section: i. Change the value of the **TCP session timeout** from the default **3600** to **60** seconds. ii. Change the value of the **TCP end timeout** from the default **20** to **5** seconds. b. In the **Out of state packets** section, you must clear all the boxes. Otherwise, the Security Group drops the traffic as out of state (because the traffic does not pass through the Security Group, it does not record the state information for the traffic).
4	From the left tree, click the **Advanced** page > click the **Configure** button, and configure: a. Click **FireWall-1** > **Stateful Inspection**. b. Clear **reject_x11_in_any**. c. Click **OK** to close the **Advanced Configuration** window.
5	Click **OK** to close the **Global Properties** window.
6	Publish the SmartConsole session.

7. **Configure the required Access Control Policy for the Virtual System in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Target* Domain Management Server that manages this Virtual System.
2	From the left navigation panel, click **Security Policies**.
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>4</td><td>Create the Access Control rule that accepts all traffic:
<table>
<tr><th>No</th><th>Name</th><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th><th>Track</th><th>Install On</th></tr>
<tr><td>1</td><td>Accept All</td><td>*Any</td><td>*Any</td><td>Any</td><td>*Any</td><td>Accept</td><td>Log</td><td>Object of Security Gateway in Monitor Mode</td></tr>
</table></td></tr>
<tr><td>5</td><td>Best Practice
We recommend these Aggressive Aging settings for the most common TCP connections:
a. In the SmartConsole, click Objects menu > Object Explorer.
b. Open Services and select TCP.
c. Search for the most common TCP connections in this network.
d. Double-click the applicable TCP service.
e. From the left tree, click Advanced.
f. At the top, select Override default settings.
On Domain Management Server, select Override global domain settings.
g. Select Match for 'Any'.
h. In the Aggressive aging section:
Select Enable aggressive aging.
Select Specific and enter 60.
i. Click OK.
j. Close the Object Explorer.</td></tr>
<tr><td>6</td><td>Publish the SmartConsole session.</td></tr>
<tr><td>7</td><td>Install the Access Control Policy on the Virtual System object.
a. Click Install Policy.
b. In the Policy field, select the applicable policy for this Virtual System object.
c. Click Install</td></tr>
</table>

Step	Instructions
8	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

8. **Make sure the Security Group enabled the Monitor Mode for Software Blades**

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.

3	Install the default policy on the VSX Gateway object:
	Make sure the parameter **fw_span_port_mode** is part of the installed policy:
	`grep -A 3 -r fw_span_port_mode $FWDIR/state/local/*`
	The returned output must show:
	`:val (true)`

9. **Connect the Security Group to the switch**

   Connect the interface in the Monitor Mode to the mirror or SPAN port on the switch.

For more information, see the:

- *Quantum Maestro Getting Started Guide*.
- *R80.20SP Quantum Maestro Gaia Administration Guide*.
- *R80.20SP Quantum Maestro VSX Administration Guide*.
- *R80.20 Security Management Administration Guide*.

Configuring Specific Software Blades for Monitor Mode

This section shows how to configure specific Software Blades for Monitor Mode.

Note - For VSX, see:

- sk79700: VSX supported features on R75.40VS and above
- sk106496: Software Blades updates on VSX R75.40VS and above - FAQ

Configuring the Threat Prevention Software Blades for Monitor Mode

Configure the settings below, if you enabled one of the Threat Prevention Software Blades (IPS, Anti-Bot, Anti-Virus, Threat Emulation or Threat Extraction) on the Security Group in Monitor Mode:

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>1</td><td>Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.</td></tr>
<tr><td>2</td><td>From the left navigation panel, click Security Policies > Threat Prevention.</td></tr>
<tr><td>3</td><td>Create the Threat Prevention rule that accepts all traffic:
<table>
<tr><th>Protected Scope</th><th>Protection/Site/File/Blade</th><th>Action</th><th>Track</th></tr>
<tr><td>*Any</td><td>-- N/A</td><td>Applicable Threat Prevention Profile</td><td>Log
Packet Capture</td></tr>
</table>
Notes:

We recommend the Optimized profile.
The Track setting Packet Capture is optional.
</td></tr>
<tr><td>4</td><td>Right-click the selected Threat Prevention profile and click Edit.</td></tr>
<tr><td>5</td><td>From the left tree, click the General Policy page and configure:
<ol type="a">
In the Blades Activation section, select the applicable Software Blades.
In the Activation Mode section:

In the High Confidence field, select Detect.
In the Medium Confidence field, select Detect.
In the Low Confidence field, select Detect.

</td></tr>
</table>

Step	Instructions
6	From the left tree, click the **Anti-Virus** page and configure: a. In the **Protected Scope** section, select **Inspect incoming and outgoing files**. b. In the **File Types** section: ■ Select **Process all file types**. ■ **Optional:** Select **Enable deep inspection scanning (impacts performance)**. c. **Optional:** In the **Archives** section, select **Enable Archive scanning (impacts performance)**.
7	From the left tree, click the **Threat Emulation** page > click **General** and configure: ■ In the **Protected Scope** section, select **Inspect incoming files from the following interfaces** and from the menu, select **All**.
8	Configure other applicable settings for the Software Blades.
9	Click **OK**.
10	Install the Threat Prevention Policy on the Security Gateway object.

For more information:

See the *R80.20 Threat Prevention Administration Guide*.

Configuring the Application Control and URL Filtering Software Blades for Monitor Mode

Configure the settings below, if you enabled Application Control or URL Filtering Software Blade on the Security Group in Monitor Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click **Manage & Settings > Blades**.
3	In the **Application Control & URL Filtering** section, click **Advanced Settings**. The **Application Control & URL Filtering Settings** window opens.
4	On the **General** page: ■ In the **Fail mode** section, select **Allow all requests (fail-open)**. ■ In the **URL Filtering** section, select **Categorize HTTPS websites**.
5	On the **Check Point online web service** page: ■ In the **Website categorization mode** section, select **Background**. ■ Select **Categorize social networking** widgets.
6	Click **OK** to close the **Application Control & URL Filtering Settings** window.
7	Install the Access Control Policy on the Security Gateway object.

For more information:

See the *R80.20 Security Management Administration Guide*.

Configuring the Data Loss Prevention Software Blade for Monitor Mode

Configure the settings below, if you enabled the Data Loss Prevention Software Blade on the Security Group in Monitor Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click **Manage & Settings > Blades**.
3	In the **Data Loss Prevention** section, click **Configure in SmartDashboard**. The SmartDashboard window opens.
4	In SmartDashboard: a. Click the **My Organization** page. b. In the **Email Addresses or Domains** section, configure with full list of company's domains. There is no need to include subdomains (for example, `mydomain.com`, `mydomain.uk`). c. In the **Networks** section, select **Anything behind the internal interfaces of my DLP gateways**. d. In the **Users** section, select **All users**.
5	Click the **Policy** page. Configure the applicable rules: ■ In the **Data** column, right-click the pre-defined data types and select **Edit**. • On the **General Properties** page, in the **Flag** field, select **Improve Accuracy**. • In the **Customer Names** data type, we recommend to add the company's real customer names. ■ In the **Action** column, you must select **Detect**. ■ In the **Severity** column, select **Critical** or **High** in all applicable rules. ■ You may choose to disable or delete rules that are not applicable to the company or reduce the Severity of these rules. **Note** - Before you can configure the DLP rules, you must configure the applicable objects in SmartConsole.

Step	Instructions
6	Click the **Additional Settings > Protocols** page. Configure these settings: ■ In the **Email** section, select **SMTP (Outgoing Emails)**. ■ In the **Web** section, select **HTTP**. Do **not** configure the **HTTPS**. ■ In the **File Transfer** section, do **not** select **FTP**.
7	Click **Launch Menu > File > Update** (or press the **CTRL S** keys).
8	Close the SmartDashboard.
9	Install the Access Control Policy on the Security Gateway object.

10	Make sure the Security Group enabled the SMTP Mirror Port Mode:
	a. Connect to the command line on the Security Group.
	b. Log in to the Expert mode.
	c. Run this command:
	`dlp_smtp_mirror_port status`
	d. Make sure the value of the kernel parameter `dlp_force_smtp_kernel_inspection` is set to 1 (one).
	Run these two commands:
	`g_fw ctl get int dlp_force_smtp_kernel_inspection`
	`g_all grep dlp_force_smtp_kernel_inspection $FWDIR/boot/modules/fwkern.conf`

For more information:

See the *R80.20 Data Loss Prevention Administration Guide*.

Configuring the Security Group in Monitor Mode Behind a Proxy Server

If you connect a Proxy Server between the Security Group in Monitor Mode and the switch, then configure these settings to see Source IP addresses and Source Users in the Security Gateway logs:

Step	Instructions
1	On the Proxy Server, configure the "**X Forward-For header**". See the applicable documentation for your Proxy Server.
2	On the Security Group in Monitor Mode, enable the stripping of the X-Forward-For (XFF) field. Follow the sk100223: How to enable stripping of X-Forward-For (XFF) field.

Deploying a Security Group in Bridge Mode

In This Section:

Introduction to Bridge Mode 418
Example Topology for Bridge Mode 419
Supported Software Blades in Bridge Mode 420
Limitations in Bridge Mode 422

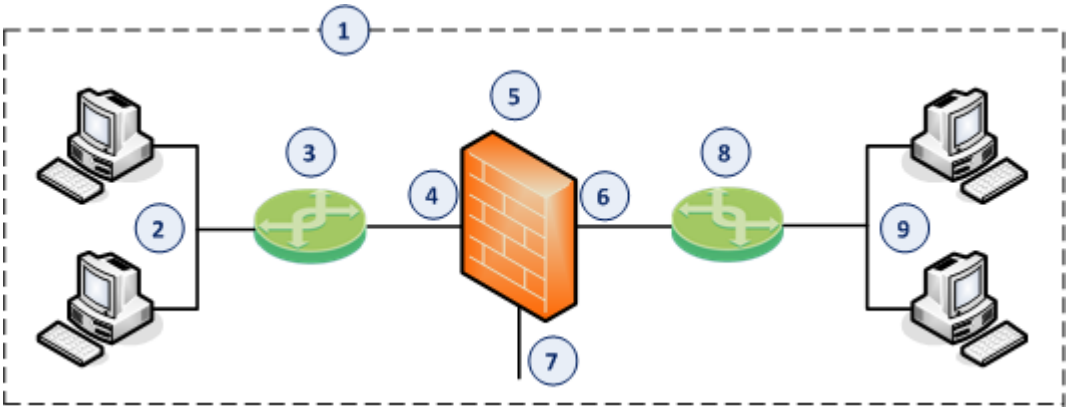
Introduction to Bridge Mode

If it is not possible divide the existing network into several networks with different IP addresses, you can configure a Security Group in the Bridge Mode.

A Security Group in Bridge Mode is invisible to Layer 3 traffic.

When traffic arrives at one of the bridge slave interfaces, the Security Group inspects it and passes it to the second bridge slave interface.

Example Topology for Bridge Mode



Item	Description
1	Network, which an administrator needs to divide into two Layer 2 segments. The Security Group in Bridge Mode connects between these segments.
2	First network segment.
3	Switch that connects the first network segment to one bridged slave interface **(4)** on the Security Group in Bridge Mode.
4	One bridged slave interface (for example, `eth1-05`) on the Security Group in Bridge Mode.
5	Security Group in Bridge Mode.
6	Another bridged slave interface (for example, `eth1-07`) on the Security Group in Bridge Mode.
7	Dedicated Gaia Management Interface (for example, `eth1-Mgmt1`) on the Security Group.
8	Switch that connects the second network segment to the other bridged slave interface **(6)** on the Security Group in Bridge Mode.
9	Second network segment.

Supported Software Blades in Bridge Mode

This table lists Software Blades, features, and their support for the Bridge Mode.

Software Blade or Feature	Support of a Security Gateway in Bridge Mode	Support of VSX Virtual Systems in Bridge Mode
Firewall	Yes	Yes
IPsec VPN	*No*	*No*
IPS	Yes	Yes
URL Filtering	Yes	Yes
DLP	Yes	No
Anti-Bot	Yes	Yes
Anti-Virus	Yes (1)	Yes (1)
Application Control	Yes	Yes
HTTPS Inspection	Yes (2)	*No*
Identity Awareness	Yes (3)	*No*
Threat Emulation - ThreatCloud emulation	Yes	Yes in Active/Active Bridge Mode *No* in Active/Standby Bridge Mode
Threat Emulation - Local emulation	Yes	*No* in all Bridge Modes

Software Blade or Feature	Support of a Security Gateway in Bridge Mode	Support of VSX Virtual Systems in Bridge Mode
Threat Emulation - Remote emulation	Yes	Yes in Active/Active Bridge Mode *No* in Active/Standby Bridge Mode
Mobile Access	*No*	*No*
UserCheck	Yes	*No*
Multi-Portal (Mobile Access Portal, Identity Awareness Captive Portal, Data Loss Prevention Portal, and so on)	Yes	*No*
QoS	Yes (see sk89581)	*No* (see sk79700)
HTTP / HTTPS proxy	Yes	*No*
Security Servers - SMTP, HTTP, FTP, POP3	Yes	*No*
Client Authentication	Yes	*No*
User Authentication	Yes	*No*

Notes:

1. Does not support the Anti-Virus in Traditional Mode.
2. HTTPS Inspection in Layer 2 works as Man-in-the-Middle, based on MAC addresses:
   - Client sends a TCP [SYN] packet to the MAC address X.
   - Security Gateway creates a TCP [SYN-ACK] packet and sends it to the MAC address X.
   - Security Gateway in Bridge Mode does not need IP addresses, because CPAS takes the routing and the MAC address from the original packet.

   Note - To be able to perform certificate validation (CRL/OCSP download), Security Gateway needs at least one interface to be assigned with an IP address. Probe bypass can have issues with Bridge Mode. Therefore, we do not recommend Probe bypass in Bridge Mode configuration.
3. Identity Awareness in Bridge Mode supports only the AD Query authentication.

Limitations in Bridge Mode

You can configure only **two** slave interfaces in one Bridge interface. You can think of this Bridge interface as a two-port Layer 2 switch. Each port can be a Physical interface, a VLAN interface, or a Bond interface.

These features and deployments are **not** supported in Bridge Mode:

- NAT rules (specifically, Firewall kernel in logs shows the traffic as accepted, but Security Gateway does not actually forward it). For more information, see sk106146.
- Access to Multi-Portal (Mobile Access Portal, Identity Awareness Captive Portal, Data Loss Prevention Portal, and so on) from bridged networks, if the bridge does not have an assigned IP address.

For more information, see sk101371: Bridge Mode on Gaia OS and SecurePlatform OS.

Configuring a Security Group in Bridge Mode

Procedure:

1. **Install the environment**

   For more information, see the *Quantum Maestro Getting Started Guide*.

Step	Instructions
1	Install the Maestro environment.
2	Configure the applicable Security Group and assign the applicable interfaces.
3	Run the Gaia First Time Configuration Wizard for the Security Group.
4	During the First Time Configuration Wizard, you must configure these settings: ■ In the **Management Connection** window, select the interface, through which you connect to Gaia operating system. ■ In the **Internet Connection** window, do not configure IP addresses. ■ In the **Installation Type** window, select **Security Gateway and/or Security Management**. ■ In the **Products** window: a. In the **Products** section, select **Security Gateway** only. b. In the **Clustering** section, clear **Unit is a part of a cluster, type**. ■ In the **Dynamically Assigned IP** window, select **No**. ■ In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

2. **Configure the Bridge interface on the Security Group**

   You configure the Bridge interface in either in Gaia Portal, or Gaia gClish of the Security Group.

   Configuring the Bridge interface in Gaia Portal

Step	Instructions
1	In the navigation tree, click **Network Management** > **Network Interfaces**.

Step	Instructions
2	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses.
3	Click **Add** > **Bridge**. To configure an existing Bridge interface, select the Bridge interface and click **Edit**.
4	On the **Bridge** tab, enter or select a **Bridge Group** ID (unique integer between 1 and 1024).
5	Select the interfaces from the **Available Interfaces** list and then click **Add**. **Notes:** ■ Make sure that the slave interfaces do not have any IP addresses or aliases configured. ■ Do **not** select the interface that you configured as Gaia Management Interface. ■ A Bridge interface in Gaia can contain only two slave interfaces.
6	On the **IPv4** tab, enter the IPv4 address and subnet mask. **Important** - R80.20SP does **not** support the option **Obtain IPv4 address automatically** (Known Limitation MBS-3246).
7	**Optional:** On the **IPv6** tab, enter the IPv6 address and mask length. **Important:** ■ First, you must enable the IPv6 Support and reboot. ■ R80.20SP does **not** support IPv6 Address on Gaia Management Interface (Known Limitation 01622840). ■ R80.20SP does **not** support the option **Obtain IPv6 address automatically** (Known Limitation MBS-3246).
8	Click **OK**.

Configuring the Bridge interface in Gaia gClish

Step	Instructions
1	Connect to the command line on the applicable Security Group.
2	Log in to Gaia Clish. Go to Gaia gClish: enter `gclish` and press Enter.

Step	Instructions

3	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned:
	`show interface <Name of Slave Interface> ipv4-address`
	`show interface <Name of Slave Interface> ipv6-address`

4	Add a new bridging group: `add bridging group <Bridge Group ID 0 - 1024>` **Note** - Do **not** change the state of bond interface manually using the "`set interface <Bridge Group ID> state`" command. This is done automatically by the bridging driver.

5	Add slave interfaces to the new bridging group:
	`add bridging group <Bridge Group ID> interface <Name of First Slave Interface>`
	`add bridging group <Bridge Group ID> interface <Name of Second Slave Interface>`
	Notes:
	■ Do **not** select the interface that you configured as Gaia Management Interface.
	■ Only Ethernet, VLAN, and Bond interfaces can be added to a bridge group.
	■ A Bridge interface in Gaia can contain only two slave interfaces.

Step	Instructions

6	Assign an IP address to the bridging group.
	Note - You configure an IP address on a Bridging Group in the same way as you do on a physical interface.
	■ To assign an IPv4 address, run:
	`set interface <Name of Bridging Group> ipv4-address <IPv4 Address> {subnet-mask <Mask> | mask-length <Mask Length>}`
	You can optionally configure the bridging group to obtain an IPv4 Address automatically.
	■ To assign an IPv6 address, run:
	`set interface <Name of Bridging Group> ipv6-address <IPv6 Address> mask-length <Mask Length>`
	You can optionally configure the bridging group to obtain an IPv6 Address automatically.
	Important - First, you must enable the IPv6 Support and reboot.

7	Save the configuration: `save config`

3. **Configure the Security Gateway object in SmartConsole**

   You can configure the Security Gateway object in either Wizard Mode, or Classic Mode.

   Configuring the Security Gateway object in Wizard Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.

Step	Instructions
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**.
4	In the **Check Point Security Gateway Creation** window, click **Wizard Mode**.
5	On the **General Properties** page: a. In the **Gateway name** field, enter the applicable name for this Security Gateway object. b. In the **Gateway platform** field, select Maestro. c. In the **Gateway IP address** section, select **Static IP address** and configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses. d. Click **Next**.
6	On the **Trusted Communication** page: a. Select the applicable option: ■ If you selected **Initiate trusted communication now**, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. ■ If you selected **Skip and initiate trusted communication later**, make sure to follow **Step 7**. b. Click **Next**.
7	On the **End** page: a. Examine the **Configuration Summary**. b. Select **Edit Gateway properties for further configuration**. c. Click **Finish**. **Check Point Gateway** properties window opens on the **General Properties** page.

Step	Instructions
8	If during the Wizard Mode, you selected **Skip and initiate trusted communication later**: a. The **Secure Internal Communication** field shows **Uninitialized**. b. Click **Communication**. c. In the **Platform** field select Maestro. d. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. e. Click **Initialize**. Make sure the **Certificate state** field shows **Established**. f. Click **OK**.
9	On the **General Properties** page, on the **Network Security** tab, enable the applicable Software Blades. **Important** - See the *Supported Software Blades in Bridge Mode* and *Limitations in Bridge Mode* sections in *"Deploying a Security Group in Bridge Mode" on page 418*.
10	On the **Network Management** page, configure the **Topology** of the Bridge interface. **Notes:** ■ If a Bridge interface connects to the Internet, then set the **Topology** to **External**. ■ If you use this Bridge Security Gateway object in Access Control Policy rules with **Internet** objects, then set the **Topology** to **External**.
11	Click **OK**.
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

Configuring the Security Gateway object in Classic Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.

Step	Instructions
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New (✳) > Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**.
4	In the **Check Point Security Gateway Creation** window, click **Classic Mode**. **Check Point Gateway** properties window opens on the **General Properties** page.
5	In the **Name** field, enter the applicable name for this Security Gateway object.
6	In the **IPv4 address** and **IPv6 address** fields, configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.
7	Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group: a. Near the **Secure Internal Communication** field, click **Communication**. b. In the **Platform** field select Maestro. c. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. d. Click **Initialize**. e. Click **OK**.

Step	Instructions

	If the **Certificate state** field does not show `Established`, perform these steps:
	a. Connect to the command line on the Security Group.
	b. Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).
	c. Run:
	`cpconfig`
	d. Enter the number of this option:
	`Secure Internal Communication`
	e. Follow the instructions on the screen to change the Activation Key.
	f. In SmartConsole, click **Reset**.
	g. Enter the same Activation Key you entered in the `cpconfig` menu.
	h. In SmartConsole, click **Initialize**.

8	In the **Platform** section, select the correct options: a. In the **Hardware** field, select Maestro. b. In the **Version** field, select **R80.20SP**. c. In the **OS** field, select **Gaia**.
9	On the **General Properties** page, on the **Network Security** tab, enable the applicable Software Blades. **Important** - See the *Supported Software Blades in Bridge Mode* and *Limitations in Bridge Mode* sections in *"Deploying a Security Group in Bridge Mode" on page 418*.
10	On the **Network Management** page, configure the **Topology** of the Bridge interface. **Notes:** ■ If a Bridge interface connects to the Internet, then set the **Topology** to **External**. ■ If you use this Bridge Security Gateway object in Access Control Policy rules with **Internet** objects, then set the **Topology** to **External**.
11	Click **OK**.

Step	Instructions
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

4. **Configure the applicable Security Policies for the Security Gateway in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click **Security Policies**.
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.
4	Create the applicable rules in the Access Control and Threat Prevention policies. **Important** - See the *Supported Software Blades in Bridge Mode* and *Limitations in Bridge Mode* sections in *"Deploying a Security Group in Bridge Mode" on page 418*.
5	Install the Access Control Policy on the Security Gateway object.
5	Install the Threat Prevention Policy on the Security Gateway object.

For more information, see the:

- *Quantum Maestro Getting Started Guide*.
- *R80.20SP Quantum Maestro Gaia Administration Guide*.
- *R80.20 Security Management Administration Guide*.
- Applicable *Administration Guides* on the R80.20 Home Page.

Accept, or Drop Ethernet Frames with Specific Protocols

By default, Security Gateway in the Bridge mode *allows* Ethernet frames that carry protocols other than IPv4 (0x0800), IPv6 (0x86DD), or ARP (0x0806) protocols.

You can configure a Security Group in the Bridge Mode to either accept, or drop Ethernet frames that carry specific protocols.

When Access Mode VLAN (VLAN translation) is configured, BPDU frames can arrive with the wrong VLAN number to the switch ports through the Bridge interface. This mismatch can cause the switch ports to enter blocking mode.

In Active/Standby Bridge Mode only, you can disable BPDU forwarding to avoid such blocking mode:

Step	Instructions
1	Connect to the command line on the applicable Security Group.
2	Log in to the Expert mode.
3	Back up the current `/etc/rc.d/init.d/network` file: `cp -v /etc/rc.d/init.d/network{,_BKP}`
4	Edit the current `/etc/rc.d/init.d/network` file: `vi /etc/rc.d/init.d/network`

5	After the line:
	`./etc/init.d/functions`
	Add this line:
	`/sbin/sysctl -w net.bridge.bpdu_ forwarding=0`

6	Save the changes in the file and exit the editor.
7	Reboot the Security Group: `reboot -b all`
8	Connect to the command line on the applicable Security Group.
9	Log in to the Expert mode.

Step	Instructions

10	Make sure the new configuration is loaded:
	`sysctl net.bridge.bpdu_forwarding`
	The expected output:
	`net.bridge.bpdu_forwarding = 0`

Routing and Bridge Interfaces

Security Gateways with a Bridge interface can support Layer 3 routing over non-bridged interfaces.

If you configure a Bridge interface with an IP address on a Security Group, the Bridge interface functions as a regular Layer 3 interface.

The Bridge interface participates in IP routing decisions on the Security Group and supports Layer 3 routing.

- Cluster deployments do not support this configuration.
- You cannot configure the Bridge interface to be the nexthop gateway for a route.
- A Security Group can support multiple Bridge interfaces, but only one Bridge interface can have an IP address.
- A Security Group cannot filter or transmit packets that it inspected before on a Bridge interface (to avoid double-inspection).

IPv6 Neighbor Discovery

Neighbor discovery works over the ICMPv6 Neighbor Discovery protocol, which is the functional equivalent of the IPv4 ARP protocol.

ICMPv6 Neighbor Discovery Protocol must be explicitly permitted in the Access Control Rule Base for all bridged networks.

This is different from ARP. ARP traffic is Layer 2 only, therefore it permitted regardless of the Rule Base.

This is an example of an explicit Rule Base that permits ICMPv6 Neighbor Discovery protocol:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On

IPv6 Neighbor Discovery	Network object that represents the Bridged Network	Network object that represents the Bridged Network	`Any`	`neighbor-advertisement`
				`neighbor-solicitation`
				`router-advertisement`
				`router-solicitation`
				`redirect6`
					`Accept`	`Log`	`Policy Targets`

Managing Ethernet Protocols

It is possible to configure a Security Gateway with bridge interface to allow or drop protocols that are not based on IP that pass through the bridge interface. For example, protocols that are not IPv4, IPv6, or ARP.

By default, these protocols are allowed by the Security Gateway.

Frames for protocols that are not IPv4, IPv6, or ARP are allowed if:

- On the Security Gateway, the value of the kernel parameter `fwaccept_unknown_protocol` is 1 (all frames are accepted)
- OR in the applicable `user.def` file on the Management Server, the protocol IS defined in the `allowed_ethernet_protocols` table.
- AND in the applicable `user.def` file on the Management Server, the protocol is NOT defined in the `dropped_ethernet_protocols` table.

To configure the Security Group to accept only specific protocols that are not IPv4, IPv6, or ARP:

Step	Instructions

1	On the Security Group, configure the value of the kernel parameter `fwaccept_unknown_protocol` to 0.
	a. Connect to the command line on the Security Group.
	b. Log in to the Expert mode.
	c. Configure the value of the kernel parameter `fwaccept_unknown_protocol` to 0:
	`g_update_conf_file fwkern.conf fwaccept_unknown_protocol=0`
	d. Reboot the Security Group.
	If the reboot is not possible at this time, then:
	■ Run this command to make the required change:
	`g_fw ctl set int fwaccept_unknown_protocol 0`
	■ Run this command to make sure the required change was accepted:
	`g_fw ctl get int fwaccept_unknown_protocol`

Step	Instructions

2	On the Management Server, edit the applicable `user.def` file.
	Note - For the list of `user.def` files, see sk98239.
	a. Back up the current applicable `user.def` file.
	b. Edit the current applicable `user.def` file.
	c. Add these directives:
	■ `allowed_ethernet_protocols` - contains the EtherType numbers (in Hex) of protocols to accept
	■ `dropped_ethernet_protocols` - contains the EtherType numbers (in Hex) of protocols to drop
	Example
	`$ifndef __user_def__`
	`$define __user_def__`
	
	`\\`
	`\\ User defined INSPECT code`
	`\\`
	
	`allowed_ethernet_protocols={`
	`<0x0800,0x86DD,0x0806>);`
	`dropped_ethernet_protocols={ <0x8137,0x8847,0x9100>`
	`);`
	
	`endif /*__user_def__*/`
	For the list of EtherType numbers, see http://standards-oui.ieee.org/ethertype/eth.csv.
	d. Save the changes in the file and exit the editor.

3	In SmartConsole, install the Access Control Policy on the Security Gateway object.

Troubleshooting

This section provides troubleshooting commands.

Note - Maestro Orchestrators do not support the Hardware Diagnostic tool that you run from the Gaia OS Boot Menu (Known Limitation MBS-17809).

Collecting System Information (asg_info)

In This Section:

Description *438*

Granularity of Commands *439*

Collected Files *439*

Syntax and Parameters *440*

Configuration Files *443*

Best Practice - Use the more advanced tool Check Point Support Data Collector (CPSDC) as described in sk164414.

Description

Use the "`asg_info`" command in Gaia gClish or the Expert mode to collect information from the .

The "`asg_info`" command collects the information from these areas:

- Log files
- Configuration files
- System status
- System diagnostics

The "`asg_info`" command saves the collected information in this file:

```
/var/log/asg_info.<Hostname>.<Date>.tar
```

By default, this command collects the information from all Security Group Members and Virtual Systems (in VSX mode).

Granularity of Commands

The "`asg_info`" command in Gaia gClish or the Expert mode executes the applicable commands with this granularity:

Source	Granularity
Security Group Members	■ All Security Group Members ■ Single Security Group Member ■ Specified Security Group Members
VSX	■ VS0 only (VSX Gateway itself) ■ For each Virtual System ■ Specified Virtual Systems

Collected Files

The "`asg_info`" command collects a predefined list of files from the Security Group Member and Virtual Systems.

A global file is located in the global folder.

Examples:

File	How the File is Collected and File Location
`latest_policy.policy.tgz`	■ Collected as a global file ■ Located in `\global\VS0\var\CPbackup\asg_backup\`
`dist_mode.log`	■ Collected from the Security Group Member and Virtual Systems folders ■ Located in `\SGM_1_01\VS1\var\log\`
`start_mbs.log`	■ Collected from the Security Group Member folder and not from the Virtual Systems folders ■ Located in `\SGM_1_01\VS0\var\log\`

Syntax and Parameters

Syntax

`asg_info -h`
`asg_info [-b <SGM IDs>] [--vs <VS IDs>] <Collect Flags> [Options]`
`asg_info [-b <SGM IDs>] [--vs <VS IDs>] [--user_conf <Path to XML Configuration File>] [Options]`

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Maestro Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Maestro Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Maestro Site (`chassis_active`) Default - Runs on all Security Group Members that are in the UP state.
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><Collect Flags></td><td>The collect flags are:
<table>
<tr><th>Flag</th><th>Instructions</th></tr>
<tr><td><code>--all</code></td><td>Collects all log files and command outputs.</td></tr>
<tr><td><code>-a</code></td><td>Collects archive files.</td></tr>
<tr><td><code>-c</code></td><td>Collects information about core dump files.</td></tr>
<tr><td><code>-f</code></td><td>Collects comprehensive log files and command outputs.</td></tr>
<tr><td><code>-i</code></td><td>Collects the "<code>cpinfo</code>" output.</td></tr>
<tr><td><code>-m | --cmm</code></td><td>This flag is not supported.</td></tr>
<tr><td><code>-q</code></td><td>Collects major log files and command outputs.</td></tr>
<tr><td><code>--user_conf <<i>Path to XML Configuration File</i>></code></td><td>Collects the specified XML configuration file.
See "Configuration Files" on page 443 below.</td></tr>
</table></td></tr>
</table>

Parameter	Description
Options	The options are: **Option** / **Instructions** `-h` — Shows the built-in help. `-e <Email_1;...;Email_N>` — Semicolon separated list of email addresses for upload notifications. `schedule` — Specifies the periodic schedule to upload report to the Check Point User Center. **Notes:** ■ This option must be the first or the last in the list of options. ■ This option asks to select the schedule (Daily, Weekly, or Monthly). ■ This option requires a valid CK (see the output of the "`cplic print`" command). ■ To see and delete the configured periodic jobs, run: `asg_info schedule` `-u` — Interactive upload of the "`asg_info`" output file to the Check Point User Center. `-uk` — Non-interactive upload of the "`asg_info`" output file to the Check Point User Center. This option requires a valid CK (see the output of the "`cplic print`" command). `-v` — Shows verbose output. `--list` — Dry run - shows all the files and command outputs to be collected without actually collecting them.

Configuration Files

File	Instructions
Default	`$FWDIR/conf/asg_info_config.xml` Files and commands are defined automatically.
User defined	You can define files and commands based on the same standard as appears in the default file.

Note - You can run the "`asg_info`" command either with the default file, or with the user-defined file. Not the two files at the same.

Example of a user-defined XML configuration file

```
<configurations>
<collect_file_list>
  <upgrade_wizard>
    <collect_mode>-f</collect_mode>
    <path>/var/log/upgrade_wizard.log*</path>
    <per_vs>0</per_vs>
    <per_sgm>1</per_sgm>
    <delete_after_collect>0</delete_after_collect>
  </upgrade_wizard>
  <active_cmm_debug>
    <collect_mode>-m</collect_mode>
    <path>/var/log/active_cmm_debug.log</path>
    <per_vs>0</per_vs>
    <per_sgm>1</per_sgm>
    <delete_after_collect>1</delete_after_collect>
  </active_cmm_debug>
</collect_file_list>
<cmd_list>
  <asg_if>
    <mode>-f</mode>
    <pre_command>g_all</pre_command>
    <command>asg if</command>
    <ipv6>0</ipv6>
    <esx>1</esx>
    <per_chassis>0</per_chassis>
    <per_vs>1</per_vs>
    <per_sgm>0</per_sgm>
    <vsx_only>0</vsx_only>
    <dest_file_name>asg_info</dest_file_name>
  </asg_if>
</cmd_list>
</configurations>
```

General Diagnostic in Security Groups

Based on the OSI model, you can run these commands:

Layer Number	Layer Name	Recommended Diagnostic Commands
7	Application	N / A

6	Presentation	■ For information about the Firewall drops, run this command in the Expert mode:
		`drop_monitor`
		See *"Packet Drop Monitoring (drop_monitor and asg_drop_monitor)" on page 258*.
		■ For information about the Firewall drops, run this command in the Expert mode:
		`g_fw ctl zdebug + drop`
		■ For information about the Software Blade Updates, run this command in the Expert mode:
		`asg_swb_update_verifier`
		■ Examine the Security Gateway logs on the Management Server or Log Server

5	Session	■ For information about the Connections table, run this command in the Expert mode:
		`g_fw tab -t connections -s`
		■ For information about the Firewall drops, run this command in the Expert mode:
		`g_fw ctl zdebug + drop`
		■ For information about the performance, run this command in Gaia gClish or the Expert mode:
		`asg perf -v -p`
		■ For information about the VSX mode, run this command:
		`asg perf -vs all -v --vvxxx`

Layer Number	Layer Name	Recommended Diagnostic Commands
4	Transport	■ For information about the Correction Layer and traffic flow, use the `g_tcpdump` command in the Expert mode ■ For information about the VPN, examine the Security Gateway logs on the Management Server or Log Server

3	Network	■ In the Expert mode, run these commands:
		• For information about the traffic:
		`asg_ifconfig`
		• For information about the routes:
		`asg_route`
		• For information about the routes:
		`asg_dr_verifier`
		• For information about the routes:
		`netstat -rn`
		• For information about the routes:
		`route`
		■ In Gaia gClish, run these commands:
		• For information about the traffic:
		`asg_ifconfig`
		• For information about the routes:
		`asg_route`
		• For information about the routes:
		`show route ...`

2	Data Link	■ For information about the Bond interfaces, run this command in Gaia gClish or the Expert mode:
		`asg_bond -v`
		■ For information about the Bridge interfaces, run this command in Gaia gClish or the Expert mode:
		`asg_br_verifier`

Layer Number	Layer Name	Recommended Diagnostic Commands

1	Physical	■ Run this command in Gaia gClish:
		`show maestro port <Port>`
		■ For information about the Bond interfaces, run this command in the Expert mode:
		`cat /proc/net/bonding/<Name of Bond Interface>`
		■ For information about the Port Link, run this command in the Expert mode:
		`ethtool ethsBP<X>-<XX>`
		■ For information about the interface statistics, run this command in the Expert mode:
		`ethtool -S ethsBP<X>-<XX>`

Configuration Verifiers

In This Section:

MAC Verification (mac_verifier) 447
Layer 2 Bridge Verifier (asg_br_verifier, asg_brs_verifier) 449
Verifying VSX Gateway Configuration (asg vsx_verify) 451

MAC Verification (mac_verifier)

You can run verifiers to make sure the configuration is correct and consistent.

Description

Each MAC address contains information about the Site ID, Security Group Member ID, and interfaces.

Use this command to make sure that the virtual MAC addresses on physical and bond interfaces are the same for all Security Group Members.

You must run this command in the Expert mode.

Syntax

```
mac_verifier -h
mac_verifier [-l] [-v]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-l`	Shows MAC address consistency on the Active Site.
`-v`	Shows information for each interface MAC Address.

Examples

Example 1

```
[Expert@MyChassis-ch0x-0x:0]# mac_verifier
-------------------------------------------------------------------------------
Collecting information from SGMs...
-------------------------------------------------------------------------------
Verifying FW1 mac magic value on all SGMs...
Success
-------------------------------------------------------------------------------
Verifying IPV4 and IPV6 kernel values...
Success
-------------------------------------------------------------------------------
Verifying FW1 mac magic value in /etc/smodb.json...
Success
-------------------------------------------------------------------------------
Verifying MAC address on local chassis (Chassis 1)...
Success
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2

```
[Expert@MyChassis-ch0x-0x:0]# mac_verifier -v
-------------------------------------------------------------------------------
Collecting information from SGMs...
-------------------------------------------------------------------------------
Verifying FW1 mac magic value on all SGMs...
FW1 mac magic value on all SGMs:
Command completed successfully

Success
-------------------------------------------------------------------------------
Verifying IPV4 and IPV6 kernel values...
IPV6 is not enabled
Success
-------------------------------------------------------------------------------
Verifying FW1 mac magic value in /etc/smodb.json...
FW1 mac magic value and /etc/smodb.json value are the same (160)
Success
-------------------------------------------------------------------------------
Verifying MAC address on local chassis (Chassis 1)...
-*- 2 blades: 1_01 1_02 -*-
BPEth0      MAC address of BPEth0 is correct

-*- 2 blades: 1_01 1_02 -*-
BPEth1      MAC address of BPEth1 is correct

-*- 2 blades: 1_01 1_02 -*-
eth1-05 00:1c:7f:81:05:a0

-*- 2 blades: 1_01 1_02 -*-
eth1-06 00:1c:7f:81:06:a0

-*- 2 blades: 1_01 1_02 -*-
eth1-07 00:1c:7f:81:07:a0

... output was truncated for brevity ...

-*- 2 blades: 1_01 1_02 -*-
eth2-64 00:1c:7f:82:40:a0

Success
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Layer 2 Bridge Verifier (asg_br_verifier, asg_brs_verifier)

Description

Use the "`asg_br_verifier`" command in Gaia gClish or the Expert mode to confirm that there are no bridge configuration problems in Virtual Systems in the Bridge Mode.

Notes:

- You must run the "`asg_br_verifier`" command in the context of the specific Virtual System in the Bridge Mode.
- This command also confirms that the "`fdb_shadow`" tables are the same for the Virtual System on different Security Group Members.
- You can run the "`asg_brs_verifier`" command in the Expert mode from the context of any Virtual System to get the output for all Virtual Systems in the Bridge Mode.

Syntax for the `asg_br_verifier` command

```
asg_br_verifier -h
asg_br_verifier [-c] [-d] [-s] [-t] [-v]
```

Syntax for the `asg_brs_verifier` command

```
asg_brs_verifier -h
asg_brs_verifier [-d] [-s] [-t] [-v]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Runs bridge verification on all Virtual Systems.
`-c`	Also shows the table entries (unformatted output).
`-d`	Shows verbose unformatted output. The "`-d`" and "`-v`" options are mutually exclusive.
`-s`	Also shows the table summary.
`-t`	Also shows the table entries (formatted output).

Parameter	Description
`-v`	Shows verbose formatted output. The "`-v`" and "`-d`" options are mutually exclusive.

Examples

Example 1 - Output in a normal state

```
[Expert@MyChassis-ch0x-0x:0]# asg_br_verifier
================================================================================
vs #3
================================================================================

Number of entries in fdb_shadow table:

-*- 10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 -*-
11

Status: OK

================================================================================
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2 - Output in a state of wrong configuration

```
[Expert@MyChassis-ch0x-0x:0]# asg_br_verifier -v
================================================================================
vs #3
================================================================================

Number of entries in fdb_shadow table:

-*- 9 blades: 1_01 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 -*-
11
-*- 1 blade: 1_02 -*-
0


Status: number of entries is different

================================================================================

Collecting table info from all SGMs. This may take a while.

Table entries in fdb_shadow table:

-*- 9 blades: 1_01 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 -*-
address="00:00:00:00:00:00" Interface="eth1-07"
address="00:10:AA:7D:08:81" Interface="eth2-07"
address="00:1E:9B:56:08:81" Interface="eth1-07"
address="00:23:FA:4E:08:81" Interface="eth1-07"
address="00:49:DC:58:08:81" Interface="eth2-07"
address="00:7E:60:77:08:81" Interface="eth1-07"
address="00:80:EA:55:08:81" Interface="eth1-07"
address="00:8D:86:52:08:81" Interface="eth2-07"
address="00:9E:8C:7F:08:81" Interface="eth1-07"
address="00:E5:DB:78:08:81" Interface="eth2-07"
address="00:E5:F7:78:08:81" Interface="eth2-07"
-*- 1 blade: 1_02 -*-
fdb_shadow table is empty
Status: Table entries in fdb_shadow table is different between SGMs

================================================================================
[Expert@MyChassis-ch0x-0x:0]#
```

Verifying VSX Gateway Configuration (asg vsx_verify)

Description

The "`asg vsx_verify`" command replaces the old verifier in the "`smo verifiers`" command and runs on a VSX system only.

Use this command to confirm that all Security Group Members have the same VSX configuration - Interfaces, Routes, and Virtual Systems.

- The same MD5 of configuration files that must be identical between Security Group Members.
- Similarity in configuration files that must be identical, but not necessarily written that way (like the `/config/active` file).

  The command uses the "`db_cleanup`" report to do this.
- The same VSX configuration on Security Group Members.
- Similarity of VMAC and BMAC addresses.

Use output when there is an inconsistency in the configuration.

The differences are compared in two ways:

- The return value of the command run on the Security Group Members with the "`gexec_inner_command`"
- The output of the commands

Example of a difference in the command output:

```
Difference between blade: 1_01 and blade: 2_01 found.
=====================================================
--- 1_01
+++ 2_01
-73b4c20e598d6b495de7515ad4ea2fdc  /opt/CPsuite-R80.20/fw1/conf/fwha_vsx_conf_id.conf
+b21dfa3feab817c3640bbb984346cdf1  /opt/CPsuite-R80.20/fw1/conf/fwha_vsx_conf_id.conf
```

When a command fails, the output contains:

```
Command "asg xxx" failed to run on blade "2_01"
```

Syntax

```
asg vsx_verify [{-a | -c | -v}]
```

Parameters

Parameter	Description
`-a`	Includes Security Group Members in the Administrative DOWN state
`-c`	Compares: ■ Database configuration between Security Group Members ■ Operating system and database configuration on each Security Group Member
`-v`	Includes Virtual Systems configuration verification table

Examples

Example 1 - 'asg vsx_verify -v'

```
> asg vsx_verify -v
+-------------------------------------------------------------------------------+
|Chassis 1 SGMs:                                                                |
|1_01 1_02 1_03                                                                 |
+-------------------------------------------------------------------------------+

+-------------------------------------------------------------------+
|VSX Global Configuration Verification                              |
+------+----------------------------------+------------------+-------+
|SGM   |VSX Configuration Signature       |Virtual Systems   |State  |
|      |VSX Configuration ID              |Installed\Allowed |       |
+------+----------------------------------+------------------+-------+
|all   |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                 |                  |       |
+------+----------------------------------+------------------+-------+

+-------------------------------------------------------------------------------+
|Virtual Systems Configuration Verification                                     |
+----+-----+-----------+---------------+----------------+---------+---------+
|VS  |SGM  |VS Name    |VS Type        |Policy Name     |SIC State|Status   |
+----+-----+-----------+---------------+----------------+---------+---------+
|0   |all  |VSX_OBJ    |VSX Gateway    |Standard        |Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|1   |all  |VSW-INT    |Virtual Switch |<Default Policy>|Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|2   |all  |VSW-INT    |Virtual Switch |<Not Applicable>|Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|3   |all  |VS-1       |Virtual System |Standard        |Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|4   |all  |VS-2       |Virtual System |Standard        |Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
Comparing Routes DB & OS. This procedure may take some time...
Press 'y' to skip this procedure...
Comparing..

+-------------------------------------------------------------------------------+
|Summary                                                                        |
+-------------------------------------------------------------------------------+
|VSX Configuration Verification completed successfully                          |
+-------------------------------------------------------------------------------+

All logs collected to /var/log/vsx_verify.1360846320.log
>
```

Example 2 - 'asg vsx_verify -a -v'

```
> asg vsx_verify -v -a
Output
+------------------------------------------------------------------------------+
|Chassis 1 SGMs:                                                               |
|1_01* 1_02 1_03 1_04                                                          |
+------------------------------------------------------------------------------+

+-------------------------------------------------------------------+
|VSX Global Configuration Verification                              |
+------+-----------------------------------+------------------+-------+
|SGM   |VSX Configuration Signature        |Virtual Systems   |State  |
|      |VSX Configuration ID               |Installed\Allowed |       |
+------+-----------------------------------+------------------+-------+
|1_01  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|1_02  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|1_03  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|1_04  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |DOWN   |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|2_01  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|2_02  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|2_03  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|2_04  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+

+------------------------------------------------------------------------------+
|Virtual Systems Configuration Verification                                    |
+----+-----+-----------+---------------+----------------+---------+---------+
|VS  |SGM  |VS Name    |VS Type        |Policy Name     |SIC State|Status   |
+----+-----+-----------+---------------+----------------+---------+---------+
|0   |all  |VSX_OBJ    |VSX Gateway    |Standard        |Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|1   |all  |VSW-INT    |Virtual Switch |<Default Policy>|Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|2   |all  |VSW-INT    |Virtual Switch |<Not Applicable>|Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|3   |all  |VS-1       |Virtual System |Standard        |Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|4   |all  |VS-2       |Virtual System |Standard        |Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
Comparing Routes DB & OS. This procedure may take some time...
Press 'y' to skip this procedure...
Comparing..

+------------------------------------------------------------------------------+
|Summary                                                                       |
+------------------------------------------------------------------------------+
|VSX Configuration Verification completed with the following errors:           |
|1. [1_02:1] eth1-06 operating system   address doesn't match                  |
|2. [1_02:1] eth1-06 DB address doesn't match                                  |
|3. [1_01:1] Found inconsistency between addresses in operating system  ,DB and NCS ofeth1-06
|
|                                                                              |
+------------------------------------------------------------------------------+
All logs collected to /var/log/vsx_verify.1360886320.log
>
```

Log and Configuration Files

This section describes some log and configuration files you can examine during the troubleshooting.

Files on Security Group Members in Security Groups

Feature	File
Additional cluster information	`$FWDIR/log/cpha_policy.log.*`
All logs that do not have a dedicated log file	`/var/log/junk.log.dbg`
Command auditing	`/var/log/asgaudit.log*`
CPD daemon	`$CPDIR/log/cpd.elg`
Discovering the hardware components	`/var/log/start_linker.log.dbg`
Distribution	`/var/log/dist_mode.log*`
Dividing physical interfaces to slave BackPlane interfaces and assembling the bond (BPEth) interfaces	`/var/log/start_tor_sgm.log.dbg` `/var/log/start_bfm.log.dbg`
Dynamic Routing	`/var/log/routed.log`
Early boot configuration cloning	`/var/log/image_clone.log.dbg`
Expert mode shell auditing	`/var/log/command_logger.log*`
FWD daemon	`$FWDIR/log/fwd.elg`
FWK daemon (VSX information)	`$FWDIR/log/fwk.elg.*` (in the context of each Virtual System)
Gaia Alerts	`/var/log/send_alert.*`
Gaia Clish auditing	`/var/log/auditlog*`
Gaia First Time Configuration Wizard	`/var/log/ftw_install.log`

Feature	File
Gaia OS installation	`/var/log/anaconda.log`
General log file	`/var/log/messages*`
Information about the dedicated Sync interfaces	`/var/log/start_smo.log.dbg`
LLDP updates	`/var/log/smartd.log.dbg` Also, run the `lldpctl` command
Log Servers	`/var/log/log_servers*`
Pulling the Security Group configuration, rebooting, cluster configuration	`$FWDIR/log/blade_config.*`
Reboot logs	`/var/log/reboot.log`
Security Group installation	`/var/log/start_mbs.log`
Silent install when adding a new Security Group Member to an existing Security Group	`/var/log/silent_install.log.dbg`
Synchronization of the new configuration to the Gaia database	`/var/log/start_smo_1.log.dbg`
VPND daemon	`$FWDIR/log/vpnd.elg*`

Files on Quantum Maestro Orchestrators

Feature	File
All logs that do not have a dedicated log file	`/var/log/junk.log.dbg`
Applying Security Group configuration	`/var/log/ssm_sg.log.dbg`
Configuring the SDK	`/var/log/messages`
Information about Security Groups	`/etc/sgdb.json`
Information about detected Security Group Members	`/etc/rsrcdb.json`
LLDP updates	`/var/log/smartd.log.dbg` Also, run the `lldpctl` command
Starting of the SDK	`/var/log/start_tor_ssm.log.dbg`

Installing the Gaia Operating System on a Quantum Maestro Orchestrator

To perform a clean installation of the Gaia Operating System on a Quantum Maestro Orchestrator, you can:

- Restore your Quantum Maestro Orchestrator to Factory Defaults.

  Note - This removes all existing configurations.

- Perform a clean install of the supported Gaia image with a bootable USB device.

Reset an Orchestrator to Factory Defaults

Important - This operation reverts the Quantum Maestro Orchestrator to the last Gaia that was installed using the Clean Install method.

Step	Instructions
1	Connect to the Quantum Maestro Orchestrator using the serial console.
2	Log in to the Gaia Clish.
3	Restart the Quantum Maestro Orchestrator. Run: `reboot`

4	During boot, press any key within 4 seconds to enter the Boot menu when you see this prompt at the top of the screen:
	`Loading the system`
	`Press any key to see the boot menu [Booting in 5 seconds]`

5	In the menu, select **Reset to factory defaults** and press Enter.
6	Type **yes** and press Enter.
7	Wait for the Quantum Maestro Orchestrator to boot.
8	With a web browser, connect to the Gaia Portal on the Quantum Maestro Orchestrator: `https://<IP Address of MGMT Port>`
9	Run the Gaia First Time Configuration Wizard.

Clean Install of the Gaia Image on an Orchestrator with a Bootable USB Device

Step	Instructions
1	Contact *Check Point Support* to configure the Quantum Maestro Orchestrator to boot from the USB device by default.
2	Download the required Clean Install package (ISO) for Maestro Orchestrators from sk138233.
3	Follow sk65205 to create a bootable USB device. **Important:** ■ Always use the latest available build of the ISOmorphic Tool. If you use an outdated build, the installation can fail. ■ Select the option **Open Server without ACPI support**.
4	Insert the bootable USB device into the Quantum Maestro Orchestrator.
5	Connect to the Quantum Maestro Orchestrator through the console port.
6	Restart the Quantum Maestro Orchestrator. Run: `reboot`
7	Wait for the Quantum Maestro Orchestrator to boot from the USB device.
8	Select the boot option **Open Server without ACPI support**.
9	Install the Gaia Operating System.
10	**Before the reboot, remove the USB device.**
11	Confirm the reboot.
12	With a web browser, connect to the Gaia Portal on the Quantum Maestro Orchestrator: `https://<IP Address of MGMT Port>`
13	Run the Gaia First Time Configuration Wizard.

Replacing a Quantum Maestro Orchestrator

Follow the steps in sk174202.

Glossary

A

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Breakout Cable
An optical fiber cable that contains several jacketed simplex optical fibers that are packaged together inside an outer jacket. Synonyms: Fanout cable, Fan-Out cable, Splitter cable.

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. See sk119715. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. For details, see sk92449.

D

DAC Cable
Direct Attach Copper cable. A form of the high-speed shielded twinax copper cable with pluggable transceivers on both ends. Used to connect to network devices (switches, routers, or servers).

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Downlink Ports
Interfaces on the Quantum Maestro Orchestrator used to connect to Check Point Security Appliances. You use DAC cables, Fiber cables (with transceivers), or Breakout cables to connect between the Downlink ports and Security Appliances. The Check Point Management traffic (policy, logs, synchronization, and so on) co-exists with the data (user) traffic on the Downlink ports. Bandwidth is guaranteed for the Check Point Management traffic (portion of the downlink bandwidth). These ports form the system backplane (management, data plane, synchronization).

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia gClish
The name of the global command line shell in Check Point Gaia operating system for Security Appliances connected to Check Point Quantum Maestro Orchestrators. Commands you run in this shell apply to all Security Appliances in the Security Group.

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

HyperSync
Check Point patented technology that makes sure that active connections are only synchronized to backup Security Appliances in the Security Group. HyperSync makes sure each connection flow has a backup within the Security Group.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Maestro Orchestrator
A scalable Network Security System that connects multiple Check Point Security Appliances into a unified system. Synonyms: Orchestrator, Quantum Maestro Orchestrator, Maestro Hyperscale Orchestrator. Acronym: MHO.

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Group
A logical group of Security Appliances that provides Active/Active cluster functionality. A Security Group can contain one or more Security Appliances. Security Groups work separately and independently from each other. To the production networks, a Security Group appears a single Security Gateway. Every Security Group contains: (A) Applicable Uplink ports, to which your production networks are connected; (B) Security Appliances (the Quantum Maestro Orchestrator determines the applicable Downlink ports automatically); (C) Applicable management port, to which the Check Point Management Server is connected.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SGM
Role of a Security Appliance (Security Gateway Module). Part of the Security Group that contains the assigned Security Appliances. A Security Appliance in a Security Group has one IPv4 address and represents all assigned Security Appliances as one entity.

Shared Management
Feature that allows to assign the same Management Port (interface ethX-MgmtY) on a Quantum Maestro Orchestrator to different Security Groups. The assigned Management Port has a different IP address and a different MAC address in each Security Group, to which this port is assigned.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

Single Management Object
Single Security Gateway object in SmartConsole that represents a Security Group configured on Quantum Maestro Orchestrator. Acronym: SMO.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

SMO Master
The physical Security Appliance in a Security Group that handles management tasks for all Security Appliances in the Security Group. By default, this role is assigned to the Security Appliance with the lowest Member ID in the Security Group.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

SSM
Role of the Quantum Maestro Orchestrator (SSM) that manages the flow of network traffic to and from the Security Groups.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

Uplink Ports
Interfaces on the Quantum Maestro Orchestrator used to connect to external and internal networks. Gaia operating system shows these interfaces in Gaia Portal and in Gaia Clish. SmartConsole shows these interfaces in the corresponding SMO Security Gateway object.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.