

Hybrid Mesh Network Security

27 May 2026

VSX

R82

Administration Guide

CHECK POINT™

Check Point Copyright Notice

© 2024 - 2026 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 R82

For more about this release, see the R82 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
27 May 2026	Updated: ■ *"VSNext" on page 19*
27 October 2025	Updated: ■ *"Configuring CoreXL on Virtual Systems" on page 143*
27 June 2025	Updated: ■ *"Working with Virtual Systems" on page 109*
21 April 2025	Updated: ■ *"CoreXL for Virtual Systems" on page 140*
17 February 2025	Updated: ■ *"vsx_util" on page 322*
22 January 2025	Updated: ■ *"VSNext" on page 19*
09 January 2025	Updated: ■ *"Changing the VSX Cluster Type" on page 208* ■ *"vsx_util convert_cluster" on page 338*
19 December 2024	Updated: ■ *"Adding a VSX Cluster" on page 368*
29 October 2024	Updated: ■ *"Licensing VSX" on page 179*
21 October 2024	First release of this document

Table of Contents

Introduction ... *16*
Example Physical Network Topology ... *16*
Example VSX Virtual Network Topology ... *17*
VSNext ... *19*
Limitations ... *19*
Introduction to VSNext ... *19*
Configuration Methods for VSNext ... *19*
Procedure for Gaia Portal ... *22*
VSX Architecture and Concepts ... *44*
Management Server Connections ... *45*
Local Management Connection ... *45*
Remote Management Connection ... *48*
VSX Management Interface ... *50*
Dedicated Management Interface (DMI) ... *50*
Non-Dedicated Management Interface (Non-DMI) ... *50*
Virtual Devices ... *51*
Interfaces ... *54*
Interface Types ... *54*
Physical Interfaces ... *55*
VLAN Interfaces ... *56*
Warp Links ... *56*
Unnumbered Interfaces ... *57*
VSX Management Overview ... *59*
Security Management Server Model ... *59*
Multi-Domain Security Management Model ... *59*
Management Model Comparison ... *62*
VSX Traffic Flow ... *64*

Overview ... 64
Context Determination ... 65
Direct Connection to a Physical Interface ... 65
Connection through a Virtual Switch ... 67
Connection through a Virtual Router ... 68
Security Enforcement ... 69
Forwarding to Destination ... 69
VSX Routing Concepts ... 70
Routing Overview ... 70
Routing Between Virtual Systems ... 70
Route Propagation ... 72
Overlapping IP Address Space ... 73
More for Virtual Switch Route Propagation ... 74
NAT ... 74
Dynamic Routing ... 75
VSX Clusters ... 76
High Availability ... 76
Virtual System Load Sharing (VSLS) ... 76
Getting Started with VSX ... **77**
Deploying VSX - Internal Network Deployment Strategies ... **79**
Security Gateway Deployment on a Physical Network ... 80
VSX Virtual System Deployment Strategies ... 81
Physical Internal Interface for Each Virtual System ... 81
Virtual Systems with Internal VLAN Interfaces ... 82
Internal Virtual Router with Source-Based Routing ... 84
Virtual Systems in Bridge Mode ... 85
Deploying VSX - Organizational Deployment Strategies ... **86**
Enterprise Deployments ... 86
Core Network Security ... 86
Dynamic Routing ... 88

Perimeter Security ... 89
Managed Service Providers Using Multi-Domain Server ... 91
Data Centers ... 93
Data Centers in an Enterprise ... 95
Configuring VSX ... **97**
Overview ... 97
Rules and Security Policies ... 97
Configuring VSX Gateways ... 98
Creating a New VSX Gateway ... 99
Wizard Step 1: Defining VSX Gateway General Properties ... 99
Wizard Step 2: Establishing SIC Trust ... 100
Initializing SIC Trust ... 100
Troubleshooting SIC Trust Initialization Problems ... 100
Troubleshooting SIC in a Scalable Platform Security Group ... 101
Wizard Step 3: Defining Physical Interfaces ... 101
Wizard Step 4: Virtual Network Device Configuration ... 102
Wizard Step 5: VSX Gateway Management ... 103
Completing the VSX Wizard ... 103
Configuring the Security Policy ... 103
Working with VSX Gateways ... 104
Changing VSX Gateway Definitions ... 104
VSX Gateway - General Properties ... 104
Secure Internal Communication (SIC) ... 105
Check Point Software Blades ... 105
VSX Gateway - Physical Interfaces ... 105
VSX Gateway - Topology ... 106
Interfaces ... 106
Routes ... 106
Topology Calculation ... 107
Deleting a VSX Gateway ... 108

Backing up and Restoring VSX Gateway ... 108
Working with Virtual Systems ... 109
Introduction ... 109
Creating a New Virtual System ... 110
Modifying a Virtual System ... 113
Configuring Bridge Interfaces in Regular Virtual Systems ... 116
Deleting a Virtual System ... 118
Configuring DNS Servers on a Virtual System ... 119
Configuring DHCP Server on a Virtual System ... 127
Working with Virtual Switches ... 128
Introduction ... 128
Creating a New Virtual Switch ... 129
Modifying a Virtual Switch ... 130
Virtual Switch - General Properties ... 130
Virtual Switch - Topology ... 130
Deleting a Virtual Switch ... 131
Working with Virtual Routers ... 132
Introduction ... 132
Creating a New Virtual Router ... 135
Modifying a Virtual Router Definition ... 135
Virtual Router - General Properties ... 136
Virtual Router - Topology ... 136
Deleting a Virtual Router ... 136
Virtual Routers in Virtual System Load Sharing Mode ... 136
Working with Source-Based Routing ... 138
Introduction ... 138
Defining Source-Based Routing Rules ... 139
CoreXL for Virtual Systems ... 140
Introduction ... 140
Configuring CoreXL on a VSX Gateway ... 141

Configuring CoreXL on a Scalable Platform Security Group ... 142
Configuring CoreXL on Virtual Systems ... 143
Dynamic Routing for Virtual Devices ... 145
Working with Interface Definitions ... 147
Adding a New Interface ... 147
Changing an Interface Definition ... 151
Deleting an Interface ... 151
Working with Authentication ... 152
Authentication Schemes ... 152
Configuring RADIUS or TACACS Authentication ... 154
Configuring RSA SecurID Authentication ... 156
Tracking the Status of VSX Objects ... 168
Working with Network Address Translation (NAT) ... 169
Configuring Application Control or URL Filtering on VSX ... 172
Configuring Threat Prevention on VSX ... 174
Licensing VSX ... 179
VSX Licenses ... 179
Upgrading Licenses ... 179
The Trial Period ... 179
Using VSX with Multi-Domain Server ... 180
VSX Provisioning ... 182
Defining Multi-Domain Servers ... 183
Working with Virtual Devices on a Multi-Domain Server ... 184
Adding a Virtual System to a Domain Management Server ... 184
Adding Virtual Routers and Virtual Switches to a Domain Management Server ... 184
Configuring VSX Clusters ... 185
VSX Cluster Overview ... 185
Physical Clusters ... 186
VSX Clusters ... 186
Planning a VSX Cluster Deployment ... 189

VSX Cluster Architecture 189
Synchronization Network 189
Internal Communication Network 190
Virtual IP Addresses 190
Working with VSX Clusters 191
Configuration Overview 191
Creating VSX Clusters 191
Modifying a VSX Cluster Definition 196
General Properties 197
VSX Cluster Members 197
Gateway VSX Cluster Member List 197
Where Used 198
Internal IP Address and Net Mask 198
ClusterXL 198
Physical Interfaces 198
Synchronization 198
Topology 199
Interfaces 199
Routes 199
Calculating Topology Automatically Based on Routing Information 201
VPN Domain 201
NAT 201
VSX Bridge Configuration 202
Changing the Cluster Management IP and/or Subnet 202
Changing the Internal Communication Network IP 203
Working with VSX Cluster Members 204
Adding a New VSX Cluster Member 204
Deleting a VSX Cluster Member 206
Changing the VSX Cluster Type 208
Converting from VSLS to High Availability 208

Converting from High Availability to VSLS ... 211
Configuring Virtual System Load Sharing (VSLS) ... 213
Introduction ... 213
Requirements ... 216
Virtual System Priority ... 216
Virtual System Weight ... 217
Virtual System States ... 217
Normalized VSLS Deployment Scenario ... 218
VSX Cluster Member Failure Scenario ... 219
Virtual System Failure Scenario ... 221
Failure Recovery ... 222
Configuring a VSX Cluster in VSLS Mode ... 223
Viewing VSLS Status ... 226
Distributing Virtual Systems Between VSX Cluster Members ... 227
Exporting and Importing VSLS Configuration ... 229
Virtual Routers in VSLS Mode ... 232
Description of Virtual Router Groups ... 232
Viewing the existing Virtual Router Groups on a Management Server ... 232
Viewing the existing Virtual Router Groups on VSX Cluster Members ... 235
VSLS Weights in Virtual Router Groups ... 235
Distributing Virtual Systems that belong to a Virtual Router Group between VSX Cluster Members ... 236
VSX Cluster in the High Availability Mode ... 237
Virtual Switches in a High Availability VSX Cluster ... 237
Advanced Clustering Configuration ... 239
Monitoring all VLANs in VSX Cluster ... 239
Configuring CoreXL in a VSLS VSX Cluster ... 239
Working with Link Aggregation ... **240**
Link Aggregation Overview ... 240
How Link Aggregation Works ... 241

Link Aggregation High Availability ... 242
Link Aggregation Load Sharing ... 243
Bond Interface Limitations ... 243
Configuring Bond High Availability Mode ... 244
Configuring the High Availability Bond ... 244
Updating the Interface Topology ... 244
Reconfiguring the Bond ... 245
Reconfiguring Topology with 'vsx_util change_interfaces' ... 246
Configuring Bond Load Sharing Mode ... 247
Configuring the Load Sharing Bond ... 247
Setting Critical Required Interfaces ... 248
Affinities of Bond Subordinate Interfaces to CPU Cores ... 248
Bond Failover ... 250
Link State Initiated Failover ... 250
Failover Initiated by Cluster Control Protocol (CCP) ... 250
Failover Support for VLANs ... 250
Configuring Cisco Switches for Link Aggregation Load Sharing Mode ... 252
For 802.3ad (LACP) ... 252
For XOR ... 252
Troubleshooting Bonded Interfaces ... 253
Troubleshooting Workflow ... 253
Connectivity Delays on Switches ... 254
Warning Regarding Use of PortFast ... 254
Optimizing VSX ... 255
Monitoring Memory Resources (vsx mstat) ... 256
Monitoring CPU Resources ... 257
SNMP Monitoring ... 258
Supported SNMP Versions ... 258
Supported SNMP Modes ... 258
SNMP Default Mode ... 259

SNMP VS Mode ... 260
SNMP VS in the "vs-direct-access" Mode ... 261
Configuring SNMP Modes ... 262
Example SNMP queries for Virtual Systems ... 264
The VSX SNMP Tree ... 267
Configuring Jumbo Frames ... 268
Jumbo Frames on a Virtual Switch ... 268
Jumbo Frames on a Virtual Router ... 269
Jumbo Frames on a Virtual System in Bridge Mode ... 269
Bridge Mode ... **270**
Active/Active Bridge Mode (Spanning Tree Protocol) ... 270
Active/Standby Bridge Mode ... 271
VLAN Shared Interface Deployment ... 271
Virtual System in Bridge Mode ... 273
Core Network Security ... 273
Configuring Virtual Systems for the Active/Standby Bridge Mode ... 275
Multi Bridge Interfaces ... 276
VSX Cluster in Bridge Mode ... 280
Enabling Active/Standby Bridge Mode on a New VSX Cluster ... 280
Enabling Active/Standby Bridge Mode on an Existing VSX Cluster ... 281
Enabling Active/Active Bridge Mode on an Existing VSX Cluster ... 282
VSX Diagnostics and Troubleshooting ... **283**
General Troubleshooting Steps ... 284
Troubleshooting Specific Problems ... 286
Command Line Reference ... **292**
Syntax Legend for CLI Commands ... 293
cpconfig ... 295
cpview ... 299
Overview of CPView ... 299
CPView User Interface ... 299

Using CPView ... 300
vsenv ... 301
vsx ... 302
vsx fetch ... 306
vsx fetch_all_cluster_policies ... 308
vsx fetchvs ... 309
vsx get ... 310
vsx mstat ... 311
vsx showncs ... 315
vsx sicreset ... 316
vsx stat ... 317
vsx unloadall ... 320
vsx vspurge ... 321
vsx_util ... 322
vsx_util add_member ... 327
vsx_util change_interfaces ... 329
vsx_util change_mgmt_ip ... 333
vsx_util change_mgmt_subnet ... 334
vsx_util change_private_net ... 336
vsx_util convert_cluster ... 338
vsx_util downgrade ... 340
vsx_util reconfigure ... 341
vsx_util remove_member ... 347
vsx_util show_interfaces ... 348
vsx_util upgrade ... 352
vsx_util view_vs_conf ... 353
vsx_util vsls ... 357
vsx_provisioning_tool ... 359
Transactions ... 362
vsx_provisioning_tool Commands ... 363

Explicit Transaction Commands ... 364
Adding a VSX Gateway ... 365
Adding a VSX Cluster ... 368
Adding a Virtual Device ... 371
Deleting a Virtual Device ... 374
Modifying Settings of a Virtual Device ... 375
Adding a Physical or VLAN Interface to a Virtual Device ... 378
Adding a Bridge Interface to a Virtual System ... 382
Adding a VPN Tunnel Interface to a Virtual Device ... 384
Removing an Interface from a Virtual Device ... 386
Modifying Settings of an Interface ... 388
Configuring a Physical Interface as VLAN Trunk ... 392
Adding a Route ... 393
Removing a Route ... 395
Showing Virtual Device Data ... 397
Script Examples ... 398
Example 1 ... 398
Example 2 ... 399
Example 3 ... 400
Configuration Examples ... ***401***
Example 1: VSX Gateway managed by Security Management Server ... 402
Topology ... 402
Action Plan ... 403
Example 2: VSX Cluster managed by Multi-Domain Server ... 414
Topology ... 415
Action Plan ... 418
Working with Kernel Parameters ... ***435***
Kernel Debug on Security Gateway ... ***436***
Glossary ... ***437***

Introduction

The VSX Administration Guide describes the **Virtual System eXtension** product that runs several virtual firewalls on the same hardware.

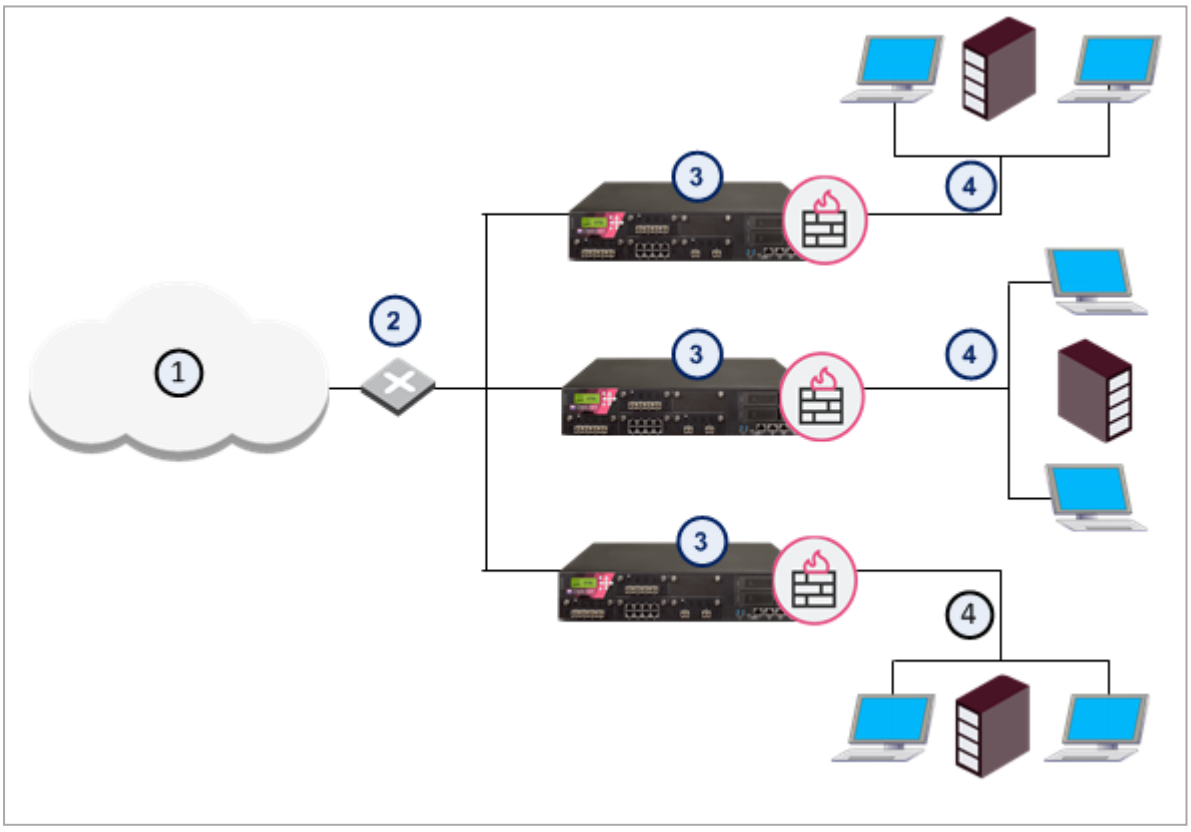
Each **Virtual System** works as a Security Gateway, typically protecting a specified network. When packets arrive at the VSX Gateway, it sends traffic to the Virtual System protecting the destination network. The Virtual System inspects all traffic and allows or rejects it according to rules defined in the security policy.

In order to better understand how virtual networks work, it is important to compare physical network environments with their virtual (VSX) counterparts. While physical networks consist of many hardware components, VSX virtual networks reside on a single configurable VSX Gateway or cluster that defines and protects multiple independent networks, together with their virtual components.

Example Physical Network Topology

In a typical deployment with multiple Security Gateways, each protects a separate network.

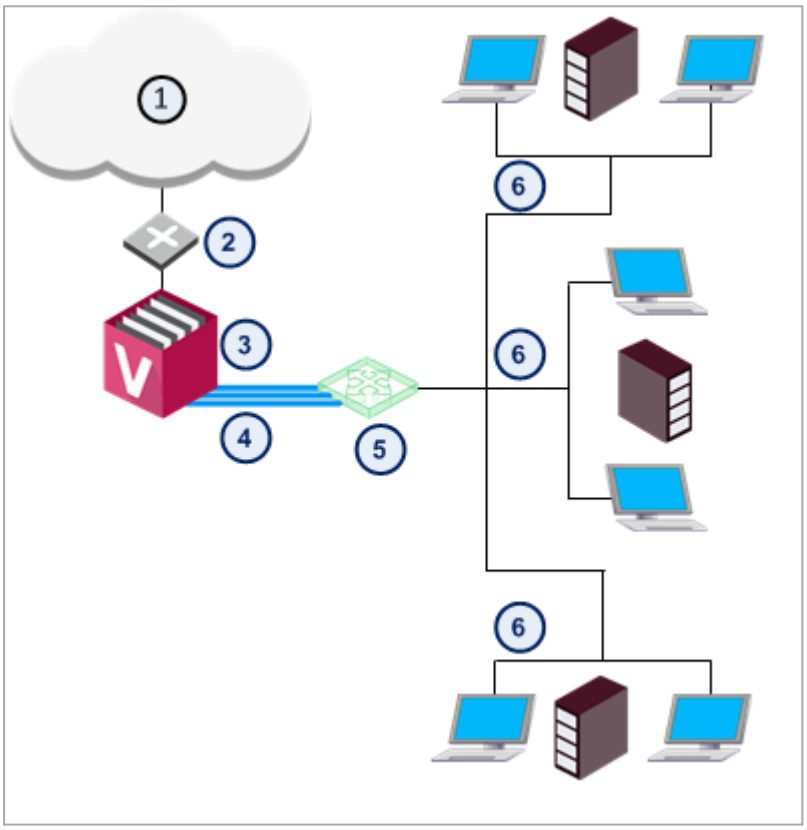
Each physical Security Gateway has interfaces to the perimeter router and to the network it protects.



Item	Description
1	Internet
2	Router
3	Security Gateways
4	Network

Example VSX Virtual Network Topology

Deploy one VSX Gateway with four Virtual Systems to protect multiple networks.



Item	Description
1	Internet
2	Router
3	VSX Gateway. Each Virtual System in a VSX environment is a Security Gateway, with the same security and networking functionality as a physical gateway. Each handles packet traffic to and from the one network it protects.

Item	Description
4	Warp Links. Virtual interfaces and network cables connect the Virtual Systems and the Virtual Switch.
5	Virtual Switch. Connects all the Virtual Systems to the Internet router.
6	Networks

VSNext

Notes:

- Starting in R82, there are two modes:
  - "VSNext" (new).
    This configuration is described below.
  - "Traditional VSX" (in versions R81.20 and lower, it is called just "VSX").
    See other chapters in this Administration Guide.
- You can enable the VSNext mode only in these:
  - ElasticXL Cluster.
  - Maestro Security Group.

  See the *R82 Scalable Platforms Administration Guide*.

Limitations

- The acceleration card hardware does not accelerate connections that pass through more than one Virtual Gateway.

Introduction to VSNext

Introduced in the R82 version, VSNext is an enhanced VSX mode that allows simpler configuration, easier provisioning, and a similar experience to a physical Security Gateway.

The benefits of the VSNext mode are:

- Unified management experience between Check Point physical Security Gateways and Virtual Gateways, including the capability to manage each Virtual Gateway from a different Management Server.
- Improves VSX provisioning performance and provisioning experience - creating, modifying, and deleting Virtual Gateways and Virtual Switches in Gaia Portal, Gaia Clish, or with Gaia REST API.
- Management feature and API parity between Virtual Gateways (VGW) and physical Security Gateways.

Important - Installation of CPUSE packages applies to the entire ElasticXL / Maestro Security Group.

Configuration Methods for VSNext

You can configure the required Virtual Gateways and Virtual Switches in one of these ways:

- **Gaia Portal:**

  Workflow

  1. Configure the required Virtual Gateways and Virtual Switches objects on the page **Virtual Systems**.
  2. In the top filter **Virtual System**, select the required Virtual Gateway.
  3. Configure the required Gaia OS settings on the available pages in Gaia Portal.

- **Gaia Clish:**

  Available Gaia Clish commands

  1. Add the required objects with these commands:

     ```
     add vsnext virtual-gateway interfaces <Name of Interface> id {auto | <1-511>} one-time-password <SIC Activation Key> instances <Number of IPv4 CoreXL Firewall Instances> instances6 Number of IPv6 CoreXL Firewall Instances wait-for-task {true | false}
     ```

     ```
     add vsnext virtual-switch name <Name of Virtual Switch> id <ID of Virtual Switch> wait-for-task {true | false}
     ```

     ```
     add vsnext virtual-link virtual-gateway <ID of Virtual Gateway> virtual-switch <ID of Virtual Switch> wrp-id <0-63>
     ```

  2. Configure the required settings with these commands:

     ```
     set vsnext interfaces <Name of Interface> virtual-system <ID of Virtual Gateway>
     ```

     ```
     set vsnext corexl-instances virtual-gateway <ID of Virtual Gateway> ipv4-instances Number of IPv4 CoreXL Firewall Instances wait-for-task {true | false}
     ```

     ```
     set vsnext corexl-instances virtual-gateway <ID of Virtual Gateway> ipv6-instances Number of IPv6 CoreXL Firewall Instances wait-for-task {true | false}
     ```

     ```
     set vsnext corexl-instances virtual-gateway <ID of Virtual Gateway> ipv4-instances Number of IPv4 CoreXL Firewall Instances ipv6-instances Number of IPv6 CoreXL Firewall Instances wait-for-task {true | false}
     ```

3. View the configured settings with these commands:

`show vsnext overview virtual-system <VS ID>`
`show vsnext overview virtual-systems`
`show vsnext recent-tasks limit <Number>`
`show vsnext running-task <Press the Tab Key to select Task ID>`
`show vsnext running-tasks`
`show vsnext state`

4. Delete the configured settings with these commands:

`delete vsnext virtual-link virtual-gateway <ID of Virtual Gateway> virtual-switch <ID of Virtual Switch>`
`delete vsnext virtual-gateway <ID of Virtual Gateway> options {skip_cpstop_on_delete | none} wait-for-task {true | false}`
`delete vsnext virtual-switch <ID of Virtual Switch> options {skip_cpstop_on_delete | none} wait-for-task {true | false}`

- **Gaia REST API:**

  In the *Check Point Gaia API Reference* (at the top, select the correct version) , or the local Gaia REST API Reference (`https://<IP Address of Gaia Management Interface>/gaia_docs/#introduction`), refer to the chapter "VSNext".

  Available API commands

1. Add the required objects with these API commands:

`add-virtual-gateway`
`add-virtual-switch`

2. Configure the required settings with these API commands:

`set-virtual-gateway`
`set-virtual-switch`

3. View the configured settings with these API commands:

`show-vsnext-state`
`show-virtual-systems`
`show-virtual-gateways`
`show-virtual-switches`
`show-virtual-gateway`
`show-virtual-switch`

4. Delete the configured settings with these API commands:

`delete-virtual-gateway`
`delete-virtual-switch`

Procedure for Gaia Portal

1. Perform a Clean Install of a supported platform and configure it as VSNext in the First Time Configuration Wizard.

   Warning - It is not supported to convert an existing platform to the VSNext mode.

   See the *R82 Release Notes* > Chapter "**Supported Environments**" > Section "**VSNext and Traditional VSX**".

   Procedure

   a. Install the required platform.

      - For an ElasticXL Cluster:

        See the *R82 Scalable Platforms Administration Guide* > Chapter "**Working with ElasticXL Cluster**".

      - For a Maestro Security Group.

        See the *Maestro Getting Started Guide*.

b. Run the First Time Configuration Wizard.

For an ElasticXL Cluster

See the *R82 Scalable Platforms Administration Guide* > Chapter "**Working with ElasticXL Cluster**".

During the First Time Configuration Wizard on the first appliance, you must configure these settings (other appliances copy these settings when they join this ElasticXL Cluster):

i. In the "**Management Connection**" window, select and configure the main Gaia Management Interface.

You connect to this IP address to open the Gaia Portal or CLI on the ElasticXL Cluster.

ii. In the **Installation Type** window, select **Security Gateway and/or Security Management**.

iii. In the **Products** window:

a. In the **Products** section, select **Security Gateway** only.

b. In the **Clustering** section, select **Unit is a part of a cluster** and select **ElasticXL**.

c. In the **Gateway Virtualization** section, select **Install as VSNext**.

iv. In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

For a Maestro Security Group

See the *R82 Scalable Platforms Administration Guide* > Chapter "**Working with Quantum Maestro**".

When you create a new Security Group on a Maestro Orchestrator, in the **First Time Wizard settings** section:

i. Enter the required hostname.

ii. Enter the required admin password.

iii. Enter the required SIC password.

iv. Select **Install as VSNext / VSX**.

c. Install a valid license.

See the *R82 Scalable Platforms Administration Guide*:

- For an ElasticXL Cluster:

  Chapter "**Working with ElasticXL Cluster**".

- For a Maestro Security Group:

  Chapter "**Working with Quantum Maestro**".

2. Connect to Gaia Portal on the ElasticXL Cluster / Maestro Security Group.

   You must connect to the same main IP address that you configured during the First Time Configuration Wizard.

3. To configure IPv6 addresses on interfaces and IPv6 CoreXL settings, you must enable the IPv6 support in Gaia OS:

   a. In the left panel, click **System Management** > **System Configuration**.

   b. In the **IPv6 Support** section, select **On**.

   c. Click **Apply**.

   d. Click **Yes** to reboot now (recommended).

   Click **No** to reboot later. Configure Virtual Gateway objects only after you reboot.

4. On the top toolbar, after the field **Virtual System**, if you see the padlock icon, then click the padlock icon, and click **Yes** to override the lock.

   The padlock icon must change to the pencil icon.

5. In the left panel, click **Virtual Systems**.

   This page shows these default predefined objects:

   - The default Virtual Switch with ID 500 (with the assigned interface "`magg1`").

     This Virtual Switch is attached to the predefined bonding group "`magg1`" that contains the port "`Mgmt`".

   - The default Virtual Gateway object with ID 0 (with the assigned interface "`wrp0`").

     The default Virtual Gateway (the interface "`wrp0`") is connected to the default Virtual Switch.

   Important - Do **not** change these default predefined objects.

6. **Optional:** Configure the default Virtual Gateway.

Best Practice - Configure the default Virtual Gateway to ensure secure access to the Gaia Operating System on the ElasticXL Cluster.

The purpose of this default Virtual Gateway is to protect the management context, to which you connect to configure other Virtual Gateways and their settings.

The main IP address of this default Virtual Gateway is the IP address you assigned to the Management Interface in the First Time Configuration Wizard.

Procedure

a. In the top panel **Virtual Systems**, click the default Virtual Gateway object with ID 0 and click **Edit**.

b. Click **Add interface**.

c. Select the checkboxes of the interfaces that you need to assign to this Virtual Gateway and click **Add**.

d. Click **OK**.

e. Monitor the progress in the bottom panel **Tasks**.

The **Status** column must show **Completed**.

For details, see these files on the ElasticXL Cluster / Maestro Security Group:

```
/var/log/vsxd.elg*
```

f. In the left panel, click **Network Management** > **Network Interfaces**.

Configure the interfaces you assigned to the default Virtual Gateway.

For more information, see the *R82 Gaia Administration Guide* > Chapter "Network Management" > Section "Network Interfaces" > Section "Physical Interfaces".

g. In the left panel, click **Network Management** > **IPv4 Static Routes**.

Add the required static routes for this Virtual Gateway.

For more information, see the *R82 Gaia Administration Guide* > Chapter "Network Management" > Section "IPv4 Static Routes".

7. Configure the required Virtual Gateways and Virtual Switches.

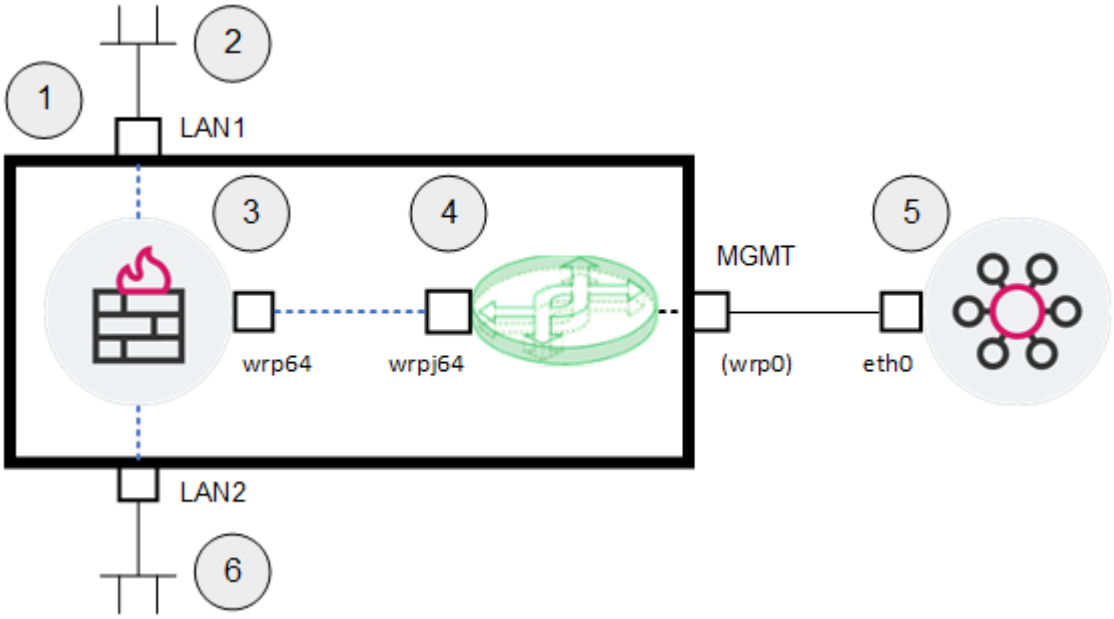
Configuration example - One Virtual Gateway managed through the default Virtual Switch

You can create many Virtual Gateways and manage all of them through the default Virtual Switch.

The IP addresses of all these Virtual Gateways must be in the same subnet as:

- The "**MGMT**" port of the ElasticXL Cluster.
- The Management port assigned to the Maestro Security Group.

Example topology:



Legend

Item	Description
1	ElasticXL Cluster in the VSNext mode.
2	Network #1 that sends traffic through the Virtual Gateway (3) to Network #2 (6).
3	Virtual Gateway that inspects traffic between Network #1 (2) and Network #2 (6). Ports **LAN1** and **LAN2** are assigned to the Virtual Gateway.
4	Default Virtual Switch that connects the Virtual Gateway (3) to the Management Server (5). ■ The Virtual Gateway connects to the Virtual Switch over an internal virtual link from `wrp64` to `wrpj64`. ■ "**MGMT**" is the name of the physical port on the Check Point appliance. ■ "**wrp0**" is the internal name of the "**MGMT**" port in the Gaia operating system.
5	Management Server that manages the Virtual Gateway (3) through its interface `wrp64`.

Legend (continued)

Item	Description
6	Network #2 that sends traffic through Virtual Gateway (3) to Network #1 (2).

Interfaces and IP addresses

Interface	IP Address / Net Mask	Description
eth0	192.168.3.57 / 24	Interface of the Management Server
wrp0	192.168.3.242 / 24	Management interface for the ElasticXL Cluster in the VSNext mode
wrp64	192.168.3.250 / 24	Management interface for the Virtual Gateway
LAN1	172.16.44.250 / 24	Interface of the Virtual Gateway that connects it to Network #1
LAN2	172.16.55.250 / 24	Interface of the Virtual Gateway that connects it to Network #2

Configuration:

a. From toolbar, click **Add** > **Virtual Gateway**.

b. In the section **Network interfaces**:

   i. Click **Add interface**.

   ii. Select the checkboxes of the interfaces that you need to assign to this Virtual Gateway.

   In our example, select **LAN1** and **LAN2**.

   iii. Click **Add**.

c. In the section **Establish trust with Management server**:

   i. In the **Activation Key** field, enter a one-time password.

      You use this password later, when you create a Security Gateway object in SmartConsole.

   ii. In the **Re-type Activation Key** field, enter the one-time password again.

   iii. In the **Interface** field, select an interface, to which you need to assign an IPv4 address.

      You use this IPv4 address later, when you create a Security Gateway object in SmartConsole.

      In our example, select: **mgmt-switch (500)**.

   iv. In the **IPv4 address** field, enter the required IPv4 address.

      In our example, enter:`192.168.3.250`

   v. In the **Mask length** field, enter the required IPv4 mask length (from 1 to 32).

      In our example, enter:`24`

   vi. In the **Default Gateway** field, enter the required IPv4 address.

      In our example, enter:`192.168.3.1`

   vii. In the **IPv6 address** field, enter the required IPv6 address.

      In our example, we do not use IPv6 addresses.

   viii. In the **Mask length** field, enter the required IPv6 mask length (from 1 to 128).

      In our example, we do not use IPv6 addresses.

   ix. In the **Default Gateway** field, enter the required IPv4 address.

      In our example, we do not use IPv6 addresses.

d. **Optional:** In the section **Advanced settings**:

   i. On the right end of the section heading, click the arrow icon to expand this section.

   ii. In the **Manually assigned VS ID** field, enter the applicable ID between 1 and 511.

   If you do not enter an ID, it is assigned automatically (the next available sequentical number).

   iii. In the **Assign IPv4 Instances** field, enter the applicable number of IPv4 CoreXL Firewall instances.

   iv. In the **Assign IPv6 Instances** field, enter the applicable number of IPv6 CoreXL Firewall instances.

e. Click **OK**.

   The popup appears with next steps. Click **OK**.

   We recommend to copy these steps and send them to yourself by email.

f. Monitor the progress in the bottom panel **Tasks**.

   The **Status** column must show **Completed**.

   For details, see these files on the ElasticXL Cluster / Maestro Security Group:

   ```
   /var/log/vsxd.elg*
   ```

g. On the top toolbar, in the field **Virtual System**, select the ID of the new Virtual Gateway.

h. In the left panel, click **Network Management** > **Network Interfaces**.

   Configure the interfaces you assigned to the Virtual Gateway:

   i. Select the interface **LAN1** > click **Edit** > configure the IPv4 address 172.16.44.250 and IPv4 Subnet mask 255.255.255.0 > click **OK**.

   ii. Select the interface **LAN2** > click **Edit** > configure the IPv4 address 172.16.55.250 and IPv4 Subnet mask 255.255.255.0 > click **OK**.

   For more information, see the *R82 Gaia Administration Guide* > chapter "Network Management" > section "Network Interfaces" > section "Physical Interfaces".

i. In the left panel, click **Network Management** > **IPv4 Static Routes**.

Add the required static routes for this Virtual Gateway.

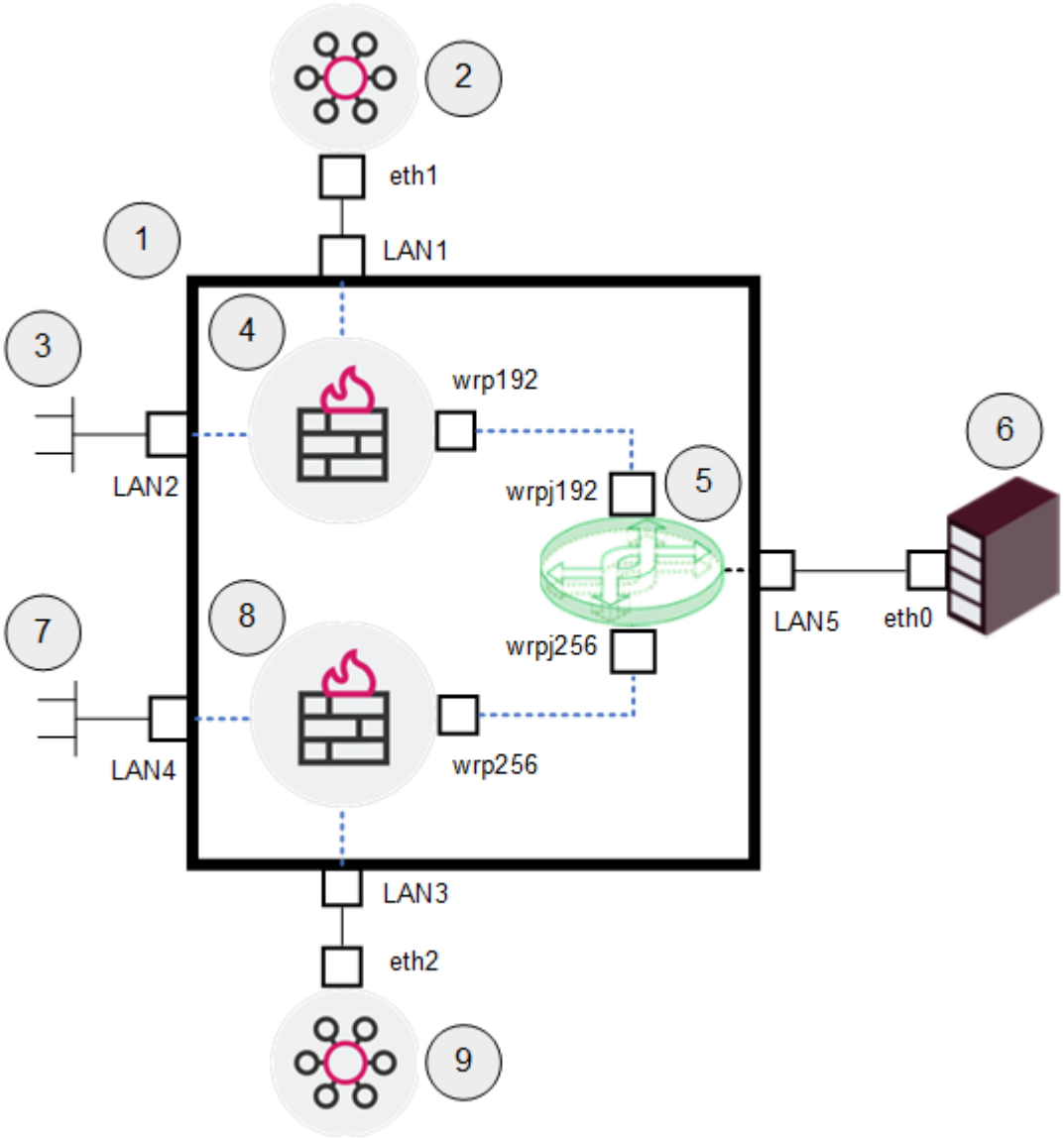
For more information, see the *R82 Gaia Administration Guide* > chapter "Network Management" > section "IPv4 Static Routes".

Configuration example - Two Virtual Gateways connect to a server through a Virtual Switch and are managed by different Management Servers

You can create many Virtual Gateways and manage each of them by different Security Management Servers / Domain Management Servers.

Each Virtual Gateway gets a unique IP address.

Example topology:



Legend

Item	Description
1	ElasticXL Cluster in the VSNext mode.
2	Management Server #1 that manages the Virtual Gateway #1 (4) through its interface **LAN1**.
3	Network #1 that sends traffic through the Virtual Gateway #1 (4) to the Backup Server (6).
4	Virtual Gateway #1 that inspects traffic between Network #1 (3) and the Backup Server (6).
5	Virtual Switch that connects the Virtual Gateway #1 (4) and the Virtual Gateway #2 (8) through the interface **LAN5** to the Server (6). ■ The Virtual Gateway #1 (4) connects over an internal virtual link from `wrp192` to `wrpj192`. ■ The Virtual Gateway #2 (8) connects over an internal virtual link from `wrp256` to `wrpj256`.
6	Backup Server, to which Network #1 (3) and Network #2 (7) send their traffic.
7	Network #2 that sends traffic through the Virtual Gateway #2 (8) to the Backup Server (6).
8	Virtual Gateway #2 that inspects traffic between Network #2 (7) and the Backup Server (6).
9	Management Server #2 that manages the Virtual Gateway #2 (8) through its interface **LAN3**.

Interfaces and IP addresses

Interface	IP Address / Net Mask	Description
eth0	10.10.10.55 / 24	Interface of the Backup Server
eth1	192.168.3.57 / 24	Interface of the Management Server #1
eth2	192.168.5.57 / 24	Interface of the Management Server #2
LAN1	192.168.3.250 / 24	Interface of the Virtual Gateway #1 that connects it to the Management Server #1
LAN2	172.16.3.250 / 24	Interface of the Virtual Gateway #1 that connects it to Network #1
wrp192	None	Interface of the Virtual Gateway #1 that connects it to the Virtual Switch
LAN3	192.168.5.250 / 24	Interface of the Virtual Gateway #2 that connects it to the Management Server #2
LAN4	172.16.5.250 / 24	Interface of the Virtual Gateway #2 that connects it to Network #2
wrp256	None	Interface of the Virtual Gateway #2 that connects it to the Virtual Switch

Configuration Part 1 - Configure Virtual Switch:

a. From toolbar, click **Add** > **Virtual Switch**.

b. In the **Name** field, enter a name for this object.

   It must start with a letter, and may contains only letters, digits, dash, and underscore.

   In our example, enter: `ServerSwitch`

c. In the **Interface** field, select an interface, to which this Virtual Switch connects.

   In our example, select **LAN5**.

d. Click **Apply**.

Configuration Part 2 - Configure Virtual Gateway #1:

a. On the top toolbar, after the field **Virtual System**, if you see the padlock icon, then click the padlock icon, and click **Yes** to override the lock.

   The padlock icon must change to the pencil icon.

b. From toolbar, click **Add** > **Virtual Gateway**.

c. In the section **Network interfaces**:

   i. Select the default interface **New connection to "mgmt-switch (500)"** and click **Remove**.

   ii. Click **Connect to Switch** > select the Virtual Switch called "`ServerSwitch`" > click **Add**.

   iii. Click **Add interface**.

   iv. Select the checkboxes of the interfaces that you need to assign to this Virtual Gateway > click **Add**.

   In our example, select **LAN1** and **LAN2**.

d. In the section **Establish trust with Management server**:

   i. In the **Activation Key** field, enter a one-time password.

      You use this password later, when you create a Security Gateway object in SmartConsole.

   ii. In the **Re-type Activation Key** field, enter the one-time password again.

   iii. In the **Interface** field, select an interface, to which you need to assign an IPv4 address.

      You use this IPv4 address later, when you create a Security Gateway object in SmartConsole.

      In our example, select: **LAN1**.

   iv. In the **IPv4 address** field, enter the required IPv4 address.

      In our example, enter:`192.168.3.250`

   v. In the **Mask length** field, enter the required IPv4 mask length (from 1 to 32).

      In our example, enter:`24`

   vi. In the **Default Gateway** field, enter the required IPv4 address.

      In our example, enter:`192.168.3.1`

   vii. In the **IPv6 address** field, enter the required IPv6 address.

      In our example, we do not use IPv6 addresses.

   viii. In the **Mask length** field, enter the required IPv6 mask length (from 1 to 128).

      In our example, we do not use IPv6 addresses.

   ix. In the **Default Gateway** field, enter the required IPv6 address.

      In our example, we do not use IPv6 addresses.

e. **Optional:** In the section **Advanced settings**:

   i. On the right end of the section heading, click the arrow icon to expand this section.

   ii. In the **Manually assigned VS ID** field, enter the applicable ID between 1 and 511.

   If you do not enter an ID, it is assigned automatically (the next available sequentical number).

   iii. In the **Assign IPv4 Instances** field, enter the applicable number of IPv4 CoreXL Firewall instances.

   iv. In the **Assign IPv6 Instances** field, enter the applicable number of IPv6 CoreXL Firewall instances.

f. Click **OK**.

   The popup appears with next steps. Click **OK**.

   We recommend to copy these steps and send them to yourself by email.

g. Monitor the progress in the bottom panel **Tasks**.

   The **Status** column must show **Completed**.

   For details, see these files on the ElasticXL Cluster / Maestro Security Group:

   ```
   /var/log/vsxd.elg*
   ```

h. On the top toolbar, in the field **Virtual System**, select the ID of the new Virtual Gateway.

i. In the left panel, click **Network Management** > **Network Interfaces**.

   Configure the interfaces you assigned to the Virtual Gateway:

   i. The interface **LAN1** already has the IPv4 address 192.168.3.250 and IPv4 Subnet mask 255.255.255.0.

   ii. Select the interface **LAN2** > click **Edit** > configure the IPv4 address 172.16.3.250 and IPv4 Subnet mask 255.255.255.0 > click **OK**.

   For more information, see the *R82 Gaia Administration Guide* > chapter "Network Management" > section "Network Interfaces" > section "Physical Interfaces".

j. In the left panel, click **Network Management** > **IPv4 Static Routes**.

   Add the required static routes for this Virtual Gateway.

   For more information, see the *R82 Gaia Administration Guide* > chapter "Network Management" > section "IPv4 Static Routes".

Configuration Part 3 - Configure Virtual Gateway #2:

a. On the top toolbar, after the field **Virtual System**, if you see the padlock icon, then click the padlock icon, and click **Yes** to override the lock.

   The padlock icon must change to the pencil icon.

b. From toolbar, click **Add** > **Virtual Gateway**.

c. In the section **Network interfaces**:

   i. Select the default interface **New connection to "mgmt-switch (500)"** and click **Remove**.

   ii. Click **Connect to Switch** > select the Virtual Switch called "`ServerSwitch`" > click **Add**.

   iii. Click **Add interface**.

   iv. Select the checkboxes of the interfaces that you need to assign to this Virtual Gateway > click **Add**.

   In our example, select **LAN3** and **LAN4**.

d. In the section **Establish trust with Management server**:

   i. In the **Activation Key** field, enter a one-time password.

      You use this password later, when you create a Security Gateway object in SmartConsole.

   ii. In the **Re-type Activation Key** field, enter the one-time password again.

   iii. In the **Interface** field, select an interface, to which you need to assign an IPv4 address.

      You use this IPv4 address later, when you create a Security Gateway object in SmartConsole.

      In our example, select: **LAN3**.

   iv. In the **IPv4 address** field, enter the required IPv4 address.

      In our example, enter:`192.168.5.250`

   v. In the **Mask length** field, enter the required IPv4 mask length (from 1 to 32).

      In our example, enter:`24`

   vi. In the **Default Gateway** field, enter the required IPv4 address.

      In our example, enter:`192.168.5.1`

   vii. In the **IPv6 address** field, enter the required IPv6 address.

      In our example, we do not use IPv6 addresses.

   viii. In the **Mask length** field, enter the required IPv6 mask length (from 1 to 128).

      In our example, we do not use IPv6 addresses.

   ix. In the **Default Gateway** field, enter the required IPv6 address.

      In our example, we do not use IPv6 addresses.

e. **Optional:** In the section **Advanced settings**:

   i. On the right end of the section heading, click the arrow icon to expand this section.

   ii. In the **Manually assigned VS ID** field, enter the applicable ID between 1 and 511.

   If you do not enter an ID, it is assigned automatically (the next available sequentical number).

   iii. In the **Assign IPv4 Instances** field, enter the applicable number of IPv4 CoreXL Firewall instances.

   iv. In the **Assign IPv6 Instances** field, enter the applicable number of IPv6 CoreXL Firewall instances.

f. Click **OK**.

   The popup appears with next steps. Click **OK**.

   We recommend to copy these steps and send them to yourself by email.

g. Monitor the progress in the bottom panel **Tasks**.

   The **Status** column must show **Completed**.

   For details, see these files on the ElasticXL Cluster / Maestro Security Group:

   ```
   /var/log/vsxd.elg*
   ```

h. On the top toolbar, in the field **Virtual System**, select the ID of the new Virtual Gateway.

i. In the left panel, click **Network Management** > **Network Interfaces**.

   Configure the interfaces you assigned to the Virtual Gateway:

   i. The interface **LAN3** already has the IPv4 address 192.168.5.250 and IPv4 Subnet mask 255.255.255.0.

   ii. Select the interface **LAN4** > click **Edit** > configure the IPv4 address 172.16.5.250 and IPv4 Subnet mask 255.255.255.0 > click **OK**.

   For more information, see the *R82 Gaia Administration Guide* > chapter "Network Management" > section "Network Interfaces" > section "Physical Interfaces".

j. In the left panel, click **Network Management** > **IPv4 Static Routes**.

Add the required static routes for this Virtual Gateway.

For more information, see the *R82 Gaia Administration Guide* > chapter "Network Management" > section "IPv4 Static Routes".

Note - You can assign additional interfaces to a Virtual Gateway later.

a. On the top toolbar, in the field **Virtual System**, select the default Virtual Gateway with ID 0.
b. In the left panel, click the **Virtual Systems** page.
c. Click the Virtual Gateway object.
d. From the top toolbar, click **Edit**.

8. On the ElasticXL Cluster / Maestro Security Group, in the context of each Virtual Gateway, configure additional applicable Gaia OS settings - Interfaces, DNS, Hosts, Static Routes, and Dynamic Routing.

   See the:

   - *R82 Gaia Administration Guide*.
   - *R82 Gaia Advanced Routing Administration Guide*.

   Each Virtual Gateway behaves as a regular Security Gateway.

   Configuration in Gaia Portal

   a. Connect to Gaia Portal on the ElasticXL Cluster / Maestro Security Group.
   b. On the top toolbar, in the field **Virtual System**, select the required Virtual Gateway.
   c. Configure the additional applicable Gaia OS settings.

   Configuration in Gaia gClish

   a. Connect to the command line on the ElasticXL Cluster / Maestro Security Group.
   b. Log in.
   c. If your default shell is the Expert mode, then go to Gaia gClish:

   ```
   gclish
   ```

   d. Go to the context of the required Virtual Gateway:

   ```
   set virtual-system <ID>
   ```

   e. Configure the additional applicable Gaia OS settings.

9. In SmartConsole, configure the Security Gateway object for each Virtual Gateway.

Configuration

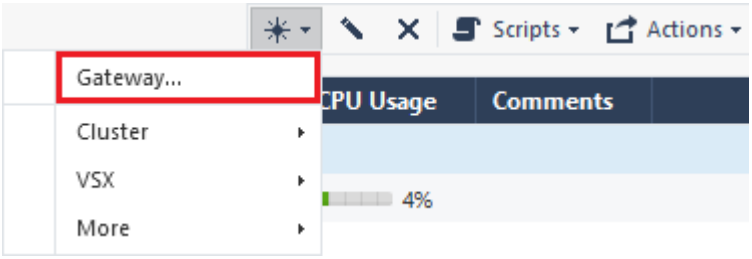
Best Practice - Configure a Security Gateway object for the **default** Virtual Gateway (with ID 0) to ensure secure access through the **"MGMT"** port.
The **default** Virtual Gateway is intended only for the management traffic.

a. Connect with SmartConsole to the Security Management Server / Domain Management Server that needs to manage the applicable Virtual Gateway.

b. From the left navigation panel, click **Gateways & Servers**.

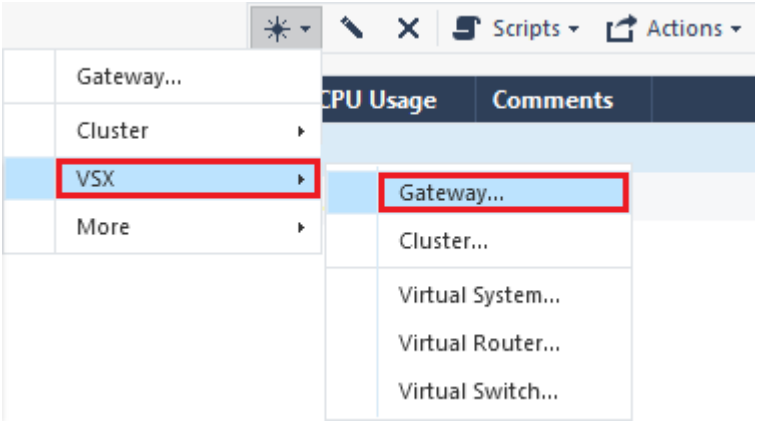
c. Create a new Security Gateway object for each Virtual Gateway:

   From the top toolbar, click **New (✳) > Gateway**:



Additional Available Options

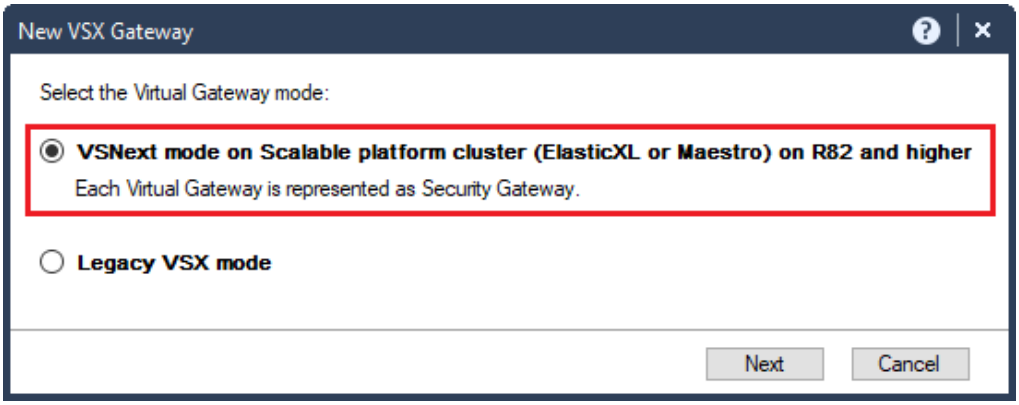
- From the top toolbar, click **New** (✳) > **VSX** > **Gateway**:



  and in the **New VSX Gateway** window:

  i. Select **VSNext mode on Scalable platform cluster (ElasticXL or Maestro) on R82 and higher**.

  ii. Click **Next**.



- In the top right corner, click the **Objects** panel > click **New** (✳) > **More** > **Network Object** > **Gateways and Servers** > **Gateway**.
- In the top right corner, click the **Objects** panel > click **New** (✳) > **More** > **Network Object** > **Gateways and Servers** > **VSX** > **Gateway** > and in the **New VSX Gateway** window:

  i. Select **VSNext mode on Scalable platform cluster (ElasticXL or Maestro) on R82 and higher**.

  ii. Click **Next**.

d. In the **Name** field, enter a desired name.

   Note - After the first policy installation, the name you assign to the Security Gateway object in SmartConsole appears in Gaia Portal of the ElasticXL Cluster / Maestro Security Group:
   - On the top toolbar, in the field **Virtual System**.
   - On the page **Virtual Systems** in the column **Name**.

e. In the **IPv4 Address** field, enter the same IPv4 address you configured for this Virtual Gateway in Gaia Portal / Gaia gClish of the ElasticXL Cluster / Maestro Security Group.

f. In the **IPv6 Address** field, enter the same IPv6 address you configured for this Virtual Gateway in Gaia Portal / Gaia gClish of the ElasticXL Cluster / Maestro Security Group.

g. Establish the Secure Internal Communication:

   i. Near the **Secure Internal Communication** field, click **Communication**.

   ii. In the **Platform** field, select **Open server / Appliance**.

   iii. Enter the same **Activation Key** you configured for this Virtual Gateway in Gaia Portal / Gaia gClish of the ElasticXL Cluster / Maestro Security Group.

   iv. Click **Initialize**.

   The **Certificate state** field must show "`Established`".

   v. Click **OK** to close the **Trusted Communication** window.

h. Make sure the Security Gateway object shows the correct values:

   i. The **Hardware** field must show:
   - For an ElasticXL Cluster, must show **ElasticXL**.
   - For a Maestro Security Group, must show **Maestro**.

   ii. The **Version** field must show **R82**.

   iii. The **OS** field must show **Gaia**.

   iv. The **Virtualization** field must show **VS**.

i. Enable and configure the required Software Blades.

   Refer to the corresponding Administration Guide on the R82 Home Page.

j. Click **OK** to close the **Check Point Gateway** window.

k. Publish the SmartConsole session.

10. In SmartConsole, configure and install the applicable Security Policies for each Virtual Gateway.

    Configuration

    Best Practice - Configure and install a Security Policy for the **default** Virtual Gateway (with ID 0) to ensure secure access.
    Allow administration access to the ElasticXL Cluster / MaestroSecurity Group and to each Virtual Gateway only from secured hosts and networks.
    The administration access requires HTTPS (for Gaia Portal) and SSH (for command line). Optionally, allow ICMP (for pings).

    a. Configure the applicable Access Control policy for each Virtual Gateway.

    b. Configure the applicable Threat Prevention policy for each Virtual Gateway.

    c. Install the Access Control policy and the Threat Prevention policy on each Virtual Gateway.

11. Add the additional required appliances to this ElasticXL Cluster / Maestro Security Group.

    The new Security Group Members automatically copy the required settings.

    See the *R82 Scalable Platforms Administration Guide*:

    - For an ElasticXL Cluster:

      Chapter "**Working with ElasticXL Cluster**".

    - For a Maestro Security Group.

      Chapter "**Working with Quantum Maestro**".

VSX Architecture and Concepts

A VSX Gateway is a physical machine that hosts virtual networks of **Virtual Devices**, with the functionality of their physical network counterparts such as Security Gateways, routers, and switches.

A VSX Gateway handles these tasks:

- Communicates with the Management Server to deploy, configure, and manage all Virtual Devices.
- Manages state synchronization for High Availability and for Load Sharing in cluster deployments.

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.

Management Server Connections

A Management Server (Security Management Server or Multi-Domain Server) connects to the VSX Gateway and provides provisioning and configuration services for Virtual Devices located on the VSX Gateway.

You can connect the Management Server to the VSX Gateway using one of the scenarios below.

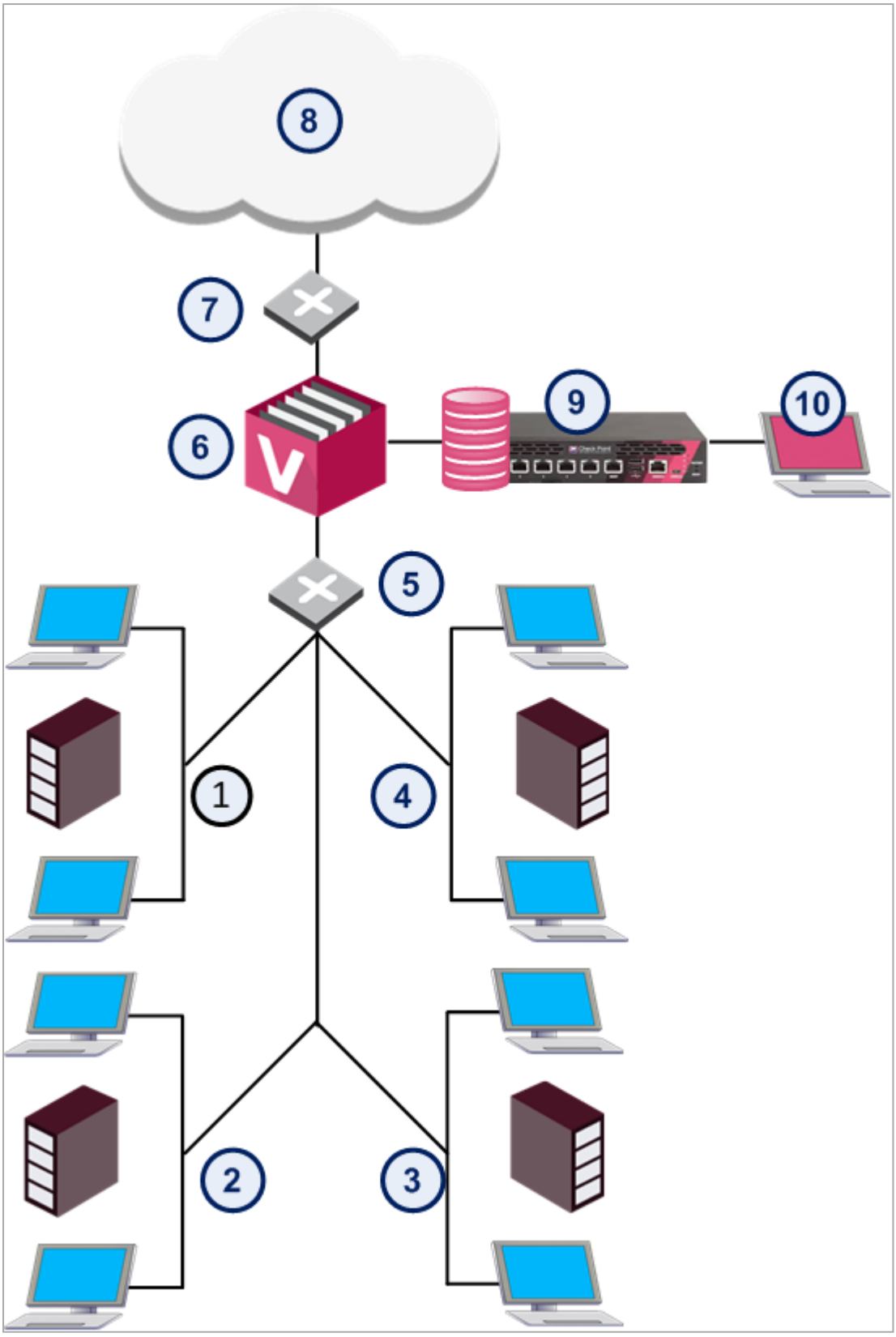
Notes:

- It is not supported to manage a VSX Gateway / VSX Cluster in these cases:
  - When the Management Server is behind NAT
  - When the VSX Gateway / VSX Cluster is behind NAT
- It is not supported to manage a VSX Gateway / VSX Cluster when the management traffic passes through a Virtual System on the same VSX Gateway / VSX Cluster.
  Only VS0 can communicate directly with the Management Server.
- From R81, configuration with a Non-Dedicated Management Interface (Non-DMI, shared interface) is deprecated and not supported.

Local Management Connection

The Management Server connects directly to the VSX Gateway using a dedicated VSX management interface.

When using a local Management Server (Security Management Server or Multi-Domain Server), all management traffic is handled by a Dedicated Management Interface (DMI) that connects the VSX Gateway to the Management Server. The IP address of this dedicated management interface can be either private or public.



Item	Description		Item	Description
1	Network 1		6	VSX Gateway

Item	Description		Item	Description
2	Network 2		7	Router
3	Network 3		8	Internet
4	Network 4		9	Management Server
5	Switch		10	SmartConsole

Remote Management Connection

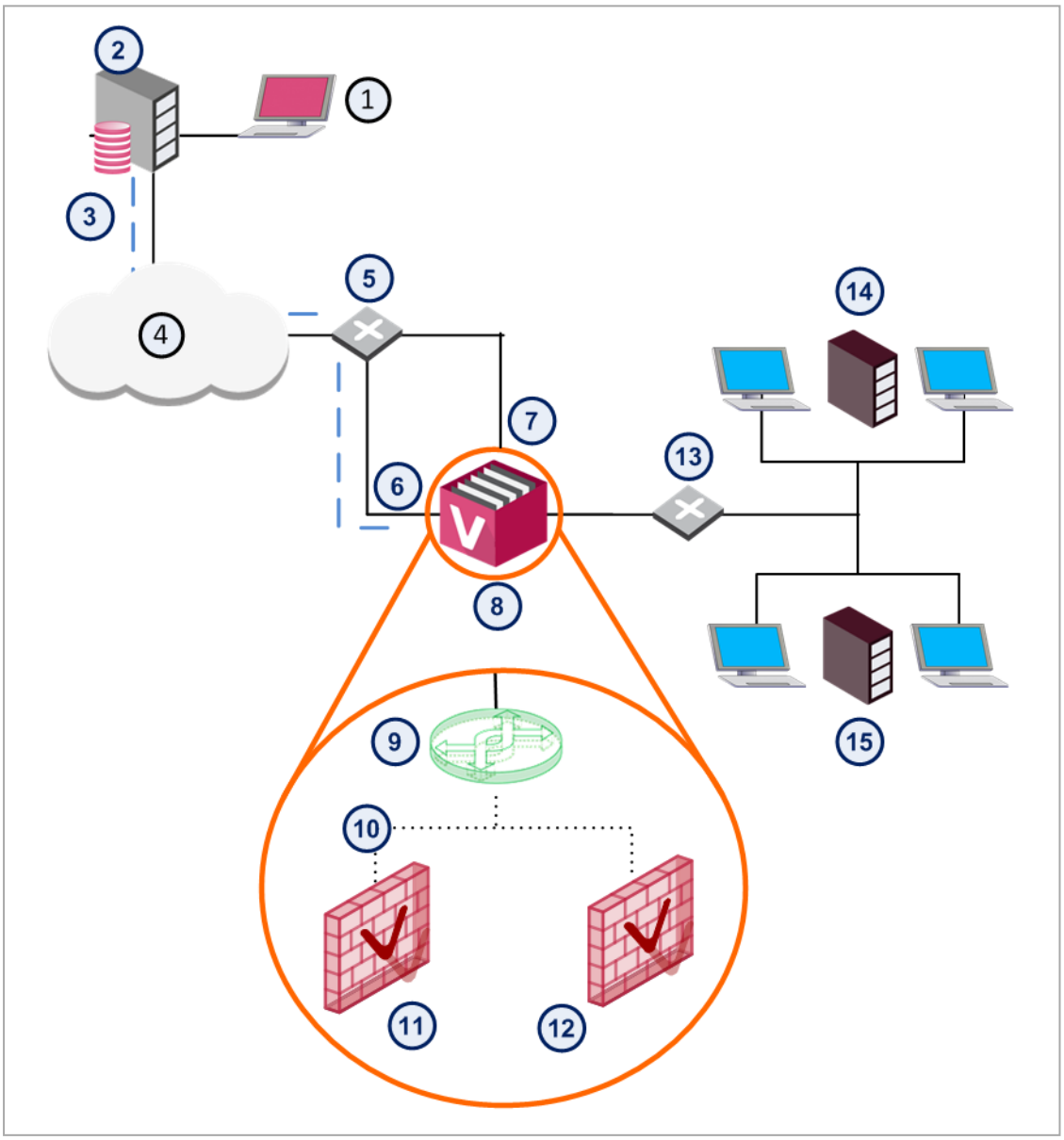
The Management Server connects to the VSX Gateway by means of a router connected to a VSX management interface.

This method ensures segregation of management traffic from all other traffic.

When using a remote Management Server (Security Management Server or Multi-Domain Server), management traffic travels via an internal or external network to a VSX Gateway to the management interface.

This architecture segregates management traffic from all other traffic passing through the VSX Gateway.

Check Point recommends that remote management connections use a dedicated management interface (DMI) that connects directly to a router or switch that leads to the external network or the Internet.



Item	Description		Item	Description
1	SmartConsole		9	Virtual Switch
2	Management Server		10	Warp Link
3	Management traffic		11	Virtual System 1
4	Internet		12	Virtual System 2
5	Router		13	Switch
6	Dedicated management interface (eth0)		14	Network 1
7	External interface		15	Network 2
8	VSX Gateway			

When management traffic passes through a Virtual Router or Virtual Switch, you must ensure that the associated Warp Link IP address originates from the remote network.

Furthermore, if the remote management connection arrives via the Internet, you must assign a routable, public IP address.

VSX Management Interface

Dedicated Management Interface (DMI)

Uses a separate interface on a VSX Gateway / VSX Cluster Members that is restricted to management traffic, such as provisioning, logging and monitoring.

Note - Dedicated Management Interface (DMI) management is not supported through a physical interface (on the VSX Gateway / VSX Cluster Members) that has one or more VLAN interfaces configured.

Best Practice - Use a DMI for management to segregate management traffic from routine "production" traffic enhanced performance, especially for end users.

Non-Dedicated Management Interface (Non-DMI)

Note - From R81, configuration with a Non-Dedicated Management Interface (Non-DMI, shared interface) is deprecated and not supported.

Virtual Devices

This section describes virtual network components and their characteristics:

Virtual Systems

A Virtual System is a virtual security and routing domain that provides the functionality of a Security Gateway with full Firewall and VPN facilities.

Multiple Virtual Systems can run concurrently on a single VSX Gateway.

Each Virtual System functions independently.

Each Virtual System maintains its own Software Blades, interfaces, IP addresses, routing table, ARP table, and dynamic routing configuration. Each Virtual System also maintains its own:

- **State Tables**: Each Virtual System has its own kernel tables with configuration and runtime data, such as active connections and IPsec tunnel information.
- **Security and VPN policies**: Each Virtual System enforces its own security and VPN Policies (including INSPECT code). Policies are retrieved from the Management Server and stored separately on the local disk and in the kernel. In a Multi-Domain Server environment, each Domain database is maintained separately on the Management Server and on the VSX Gateway.
- **Configuration Parameters**: Each Virtual System maintains its own configuration, such as IPS settings and TCP/UDP time-outs. Different Virtual Systems can run in Layer 2 or Layer 3 mode and co-exist on the same VSX Gateway.
- **Logging Configuration**: Each Virtual System maintains its own logs and runs logging according to its own rules and configuration.

Virtual Routers

Note - Security Groups in Maestro and Scalable Chassis do not support Virtual Routers (Known Limitation 01413513).

A **Virtual Router** is an independent routing domain within a VSX Gateway that performs the functionality of physical routers.

Virtual Routers are useful for connecting multiple Virtual Systems to a shared interface, such as the interface leading to the Internet, and for routing traffic from one Virtual System to another. Virtual Routers support dynamic routing.

Virtual Routers perform the following routing functions:

- Packets arriving at the VSX Gateway through a shared interface to the designated Virtual System based on the source or destination IP address.
- Traffic arriving from Virtual Systems directed to a shared interface or to other Virtual Systems.
- Traffic to and from shared network resources such as a DMZ.

As with physical routers, each Virtual Router maintains a routing table with a list of route entries describing known networks and directions on how to reach them.

Depending on the deployment requirements, multiple Virtual Routers can be configured.

To protect themselves, Virtual Routers inspect all traffic destined to, or emanating from themselves (for example, an ICMP ping to the Virtual Router IP address) based on the security policy. Traffic that is not sent to, or coming from the Virtual Router is not inspected by the Virtual Router policy and is sent to its destination.

Virtual Switches

By providing Layer 2 connectivity, a **Virtual Switch** connects Virtual Systems and facilitates sharing a common physical interface without segmenting the existing IP network. As with a physical switch, each Virtual Switch maintains a forwarding table with a list of MAC addresses and their associated ports.

In contrast to a Virtual Router, when sharing a physical interface via a Virtual Switch there is no need:

- To allocate an additional subnet for IP addresses of Virtual Systems connected to the switch.
- To manually configure the routing on the routers adjacent to the shared interface.

You can create multiple Virtual Switches in a virtual network topology.

Note - When sharing a physical interface via a Virtual Switch, the IP addresses for Virtual Systems connected to a Virtual Switch should be allocated from the same subnet as the shared interface. If the only function the Virtual Switch performs is to connect Virtual Systems, then the Virtual Switch can be defined without interfaces (unless Virtual System Load Sharing is enabled).

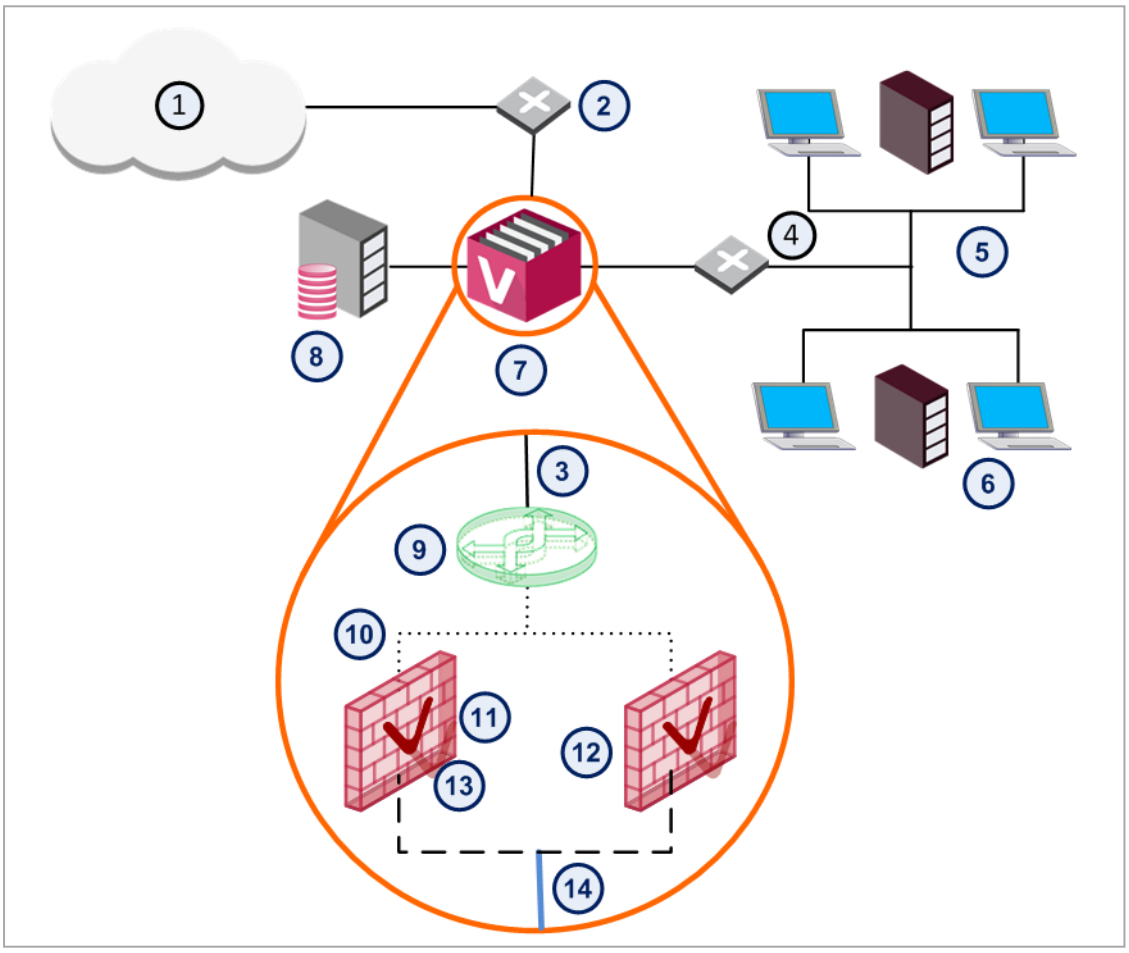
Interfaces

This section describes the various types of interfaces and how they are used in a VSX configuration.

Interface Types

The principal interface types are:

- Physical Interface
- VLAN interface
- Warp Link (including unnumbered interfaces)



Item	Description		Item	Description
1	Internet		8	Management Server
2	Router		9	Virtual Switch
3	Physical interface		10	Warp interface

Item	Description		Item	Description
4	VLAN Switch		11	Virtual System 1
5	Network 1		12	Virtual System 2
6	Network 2		13	VLAN Interface
7	VSX Gateway		14	VLAN Trunk

Notes:

- Warp Links connect the Virtual Switch to each Virtual System.
- A Physical Interface connects the Virtual Switch to an external router leading to the Internet.
- VLAN Interfaces connect the Virtual Systems to the VLAN Switch, through a VLAN Trunk.
- The VLAN switch connects to the protected networks.

Physical Interfaces

Physical interfaces connect a VSX Gateway to Management Server and to internal and external networks.

There are different types of physical interfaces used in a VSX Gateway:

- **Dedicated Management Interface**: Connects the VSX Gateway to the Management Server when it is locally managed.

  If the VSX Gateway is remotely managed, the management connection arrives through the external or internal interface.

- **External interface**: Connects the VSX Gateway to the Internet or other untrusted networks.
- **Internal Interface**: Connects the VSX Gateway to a protected network.
- **Synchronization Interface**: Connects one VSX Cluster Member to other VSX Cluster Members for state synchronization.

You can install and configure more physical interfaces to a Virtual Device as required.

A VSX Gateway can theoretically contain as many physical interfaces as permitted by VSX Gateway hardware and memory constraints.

VLAN Interfaces

Virtual Systems typically connect to protected VLAN networks using IEEE 802.1q compliant VLAN Interfaces.

The networks are connected to ports on an 802.1q-compliant switch that trunks all traffic via a single physical interface to the VSX Gateway.

VSX uses VLAN tags to direct the Ethernet frames to the specific Virtual System handling each network.

VSX assigns a virtual VLAN interface to each VLAN tag on a specific physical interface.

For example: VLAN tag 100 on *eth3* will be assigned a virtual interface named *eth3.100*.

Warp Links

Note - Security Groups in Maestro and Scalable Chassis do not support Virtual Routers (Known Limitation 01413513).

A Warp Link is a virtual point-to-point connection between a Virtual System and a Virtual Router or Virtual Switch.

Each side of a Warp Link represents a virtual interface with the appropriate Virtual Device.

VSX automatically assigns a name to each virtual interface when administrators create the link.

Warp Interfaces on the Virtual System side are assigned the prefix `wrp` and those on the Virtual Router / Virtual Switch side are assigned the prefix `wrpj`.

In both cases, VSX appends a unique number to the prefix to form the interface name.

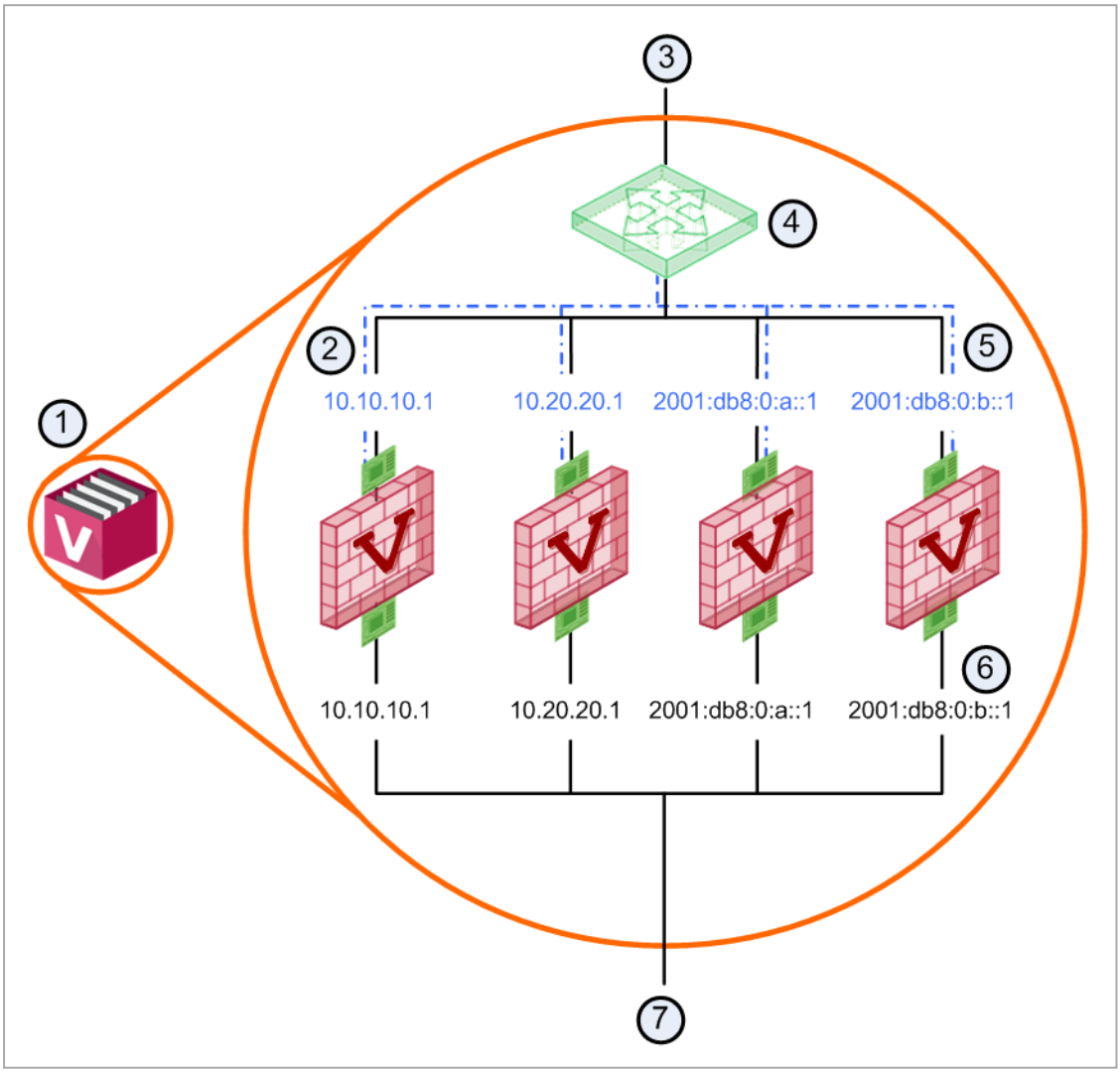
When connected to a Virtual Switch, VSX also assigns a unique MAC address to each Warp Link.

Unnumbered Interfaces

VSX lets you reduce the number of IP addresses required for a VSX network deployment when using one or more Virtual Routers.

A Warp Link connected to a Virtual Router can "borrow" an existing IP address from another interface, instead of assigning a dedicated address to the interface leading to a Virtual Router.

This capability is known as an **Unnumbered Interface**.



Item	Description
1	VSX Gateway
2	The external interface serves as the next hop from the Virtual Router
3	External
4	Virtual Router

Item	Description
5	Unnumbered External Interfaces IP "borrowed" from internal interfaces
6	Internal Interfaces with predefined IP addresses
7	Internal

In this example, the external interfaces for each Virtual System are unnumbered and borrow the IP address of the internal interfaces.

Unnumbered interfaces act as the next hop from the Virtual Router.

Unnumbered Interface Limitations

The following limitations apply to Unnumbered Interfaces:

- Unnumbered interfaces must connect to a Virtual Router.
- You can only "borrow" an individual interface IP address once.
- In order to use VPN or Hide NAT, the borrowed address must be routable.

VSX Management Overview

VSX supports two Check Point management models: Security Management Server and Multi-Domain Server.

Both models provide central configuration, management and monitoring for multiple VSX Gateways and Virtual Systems.

The choice of management model depends on several factors, including:

- The scale of the current deployment and anticipated expansion
- Administrative requirements
- Physical and operational requirements
- Licensing restrictions

You can use either management model to manage a "physical" Security Gateway together with a VSX Gateway and Virtual Systems.

You can also manage VPN communities and remote connections with either model.

Note - According to the Check Point EULA (End User License Agreement), a Security Gateway can only manage security policies for Virtual Systems belonging to a single legal entity. In order to manage Virtual Systems belonging to multiple legal entities, you need to deploy a Multi-Domain Security Management solution with a separate Domain Management Server for each legal entity. For more information regarding Licensing, refer to your Check Point Reseller.

Security Management Server Model

The Security Management Server model is for enterprise deployments with many Virtual Systems, but one domain.

SmartConsole connects to the VSX Gateway, which contains the Virtual Systems, and directly manages each Virtual System.

Multi-Domain Security Management Model

With Multi-Domain Security Management, you centrally manage multiple networks, typically of different Domains, divisions, or branches.

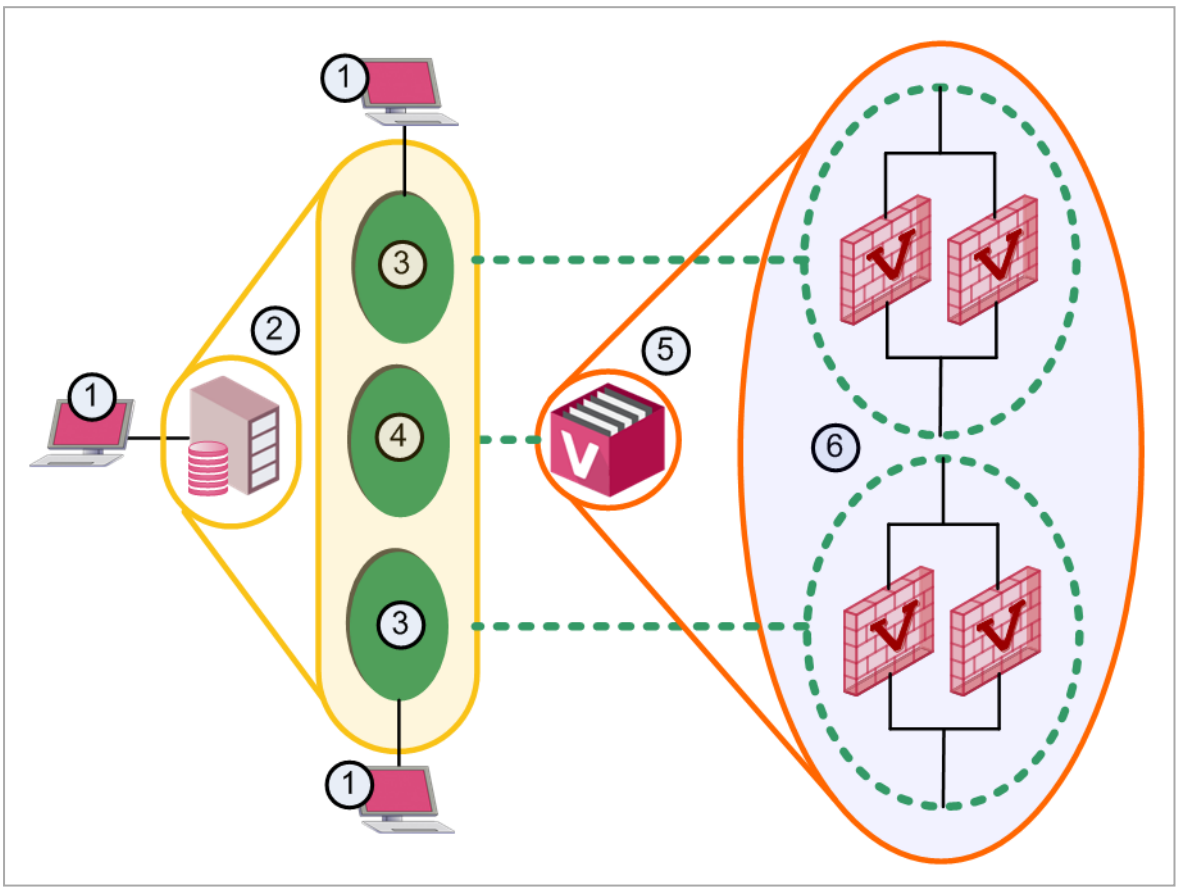
The **Multi-Domain Server** is the central management node that controls the policy databases for each of these networks.

Each Domain network is managed by a **Domain Management Server**, which provides the full functionality of a Security Management Server and can host multiple Virtual Systems, virtual and physical devices.

The Domain Management Server that manages a VSX Gateway or VSX Cluster is the **Main** Domain Management Server.

A VSX Gateway or VSX Cluster can host Virtual Systems that are managed by different Domain Management Servers.

The Domain Management Server that manages a VSX Virtual System or VSX Virtual Router is the **Target** Domain Management Server.



Item	Description
1	SmartConsole
2	Multi-Domain Server
3	Domain Management Server
4	Main Domain Management Server
5	VSX Gateway
6	Virtual Systems in Domain Management Servers

From a SmartConsole connected to a Multi-Domain Server, provision and configure Domains and Domain Management Servers.

Each Domain Management Server uses its own SmartConsole instance to provision and configure its Virtual Systems, Virtual Devices, and policies.

Management Model Comparison

The following table summarizes the capabilities and differences between the two management models.

The capacity figures shown for Multi-Domain Server represent estimated, practical limits that will sustain acceptable performance levels under normal conditions.

Actual performance is dependent on many factors, including deployed hardware, network topology, traffic load and security requirements.

Feature	Security Management Server	Multi-Domain Server (Practical Limit)
Management Domains	1	250
Concurrent Administrators	1	250
Object Databases	1	250
Policies	250	250
Certificate Authorities	1	250
Virtual Systems	25 (recommended)	250

Management Server Communication - SIC

All communication between the Management Server and the VSX Gateway is accomplished by means of Secure Internal Communication (SIC), a certificate based channel that authenticates communication between Check Point components.

The Management Server uses SIC for provisioning Virtual Devices, policy installation, logging, and status monitoring.

SIC trust is initially established using a one-time password during configuration of the VSX Gateway or VSX Cluster Members.

For Multi-Domain Security Management deployments, SIC trust is established between the Domain Management Server associated with the VSX Gateway or VSX Cluster (Main Domain Management Server).

The Virtual Devices establish trust in a different manner than their physical counterparts.

When you create a Virtual Device, VSX automatically establishes the SIC trust using the secure communication channel defined between the Management Server and the VSX Gateway.

The VSX Gateway uses its management interface for Secure Internal Communication between the Management Server and all Virtual Devices.

VSX Traffic Flow

In This Section:

Overview 64

Context Determination 65

Direct Connection to a Physical Interface 65

Connection through a Virtual Switch 67

Connection through a Virtual Router 68

Security Enforcement 69

Forwarding to Destination 69

Overview

A VSX Gateway processes traffic according to the following steps:

- Context determination
- Security enforcement
- Forwarding to destination

Context Determination

VSX incorporates **VRF** (Virtual Routing and Forwarding) technology that allows creation of multiple, independent routing domains on a single VSX Gateway or VSX Cluster. The independence of these routing domains makes possible the use of Virtual Devices with overlapping IP addresses. Each routing domain is known as a **context**.

When traffic arrives at a VSX Gateway, a process known as **Context Determination** directs traffic to the appropriate Virtual System, Virtual Router or Virtual Switch. The context determination process depends on the virtual network topology and the connectivity of the Virtual Devices.

The basic Virtual System connection scenarios are:

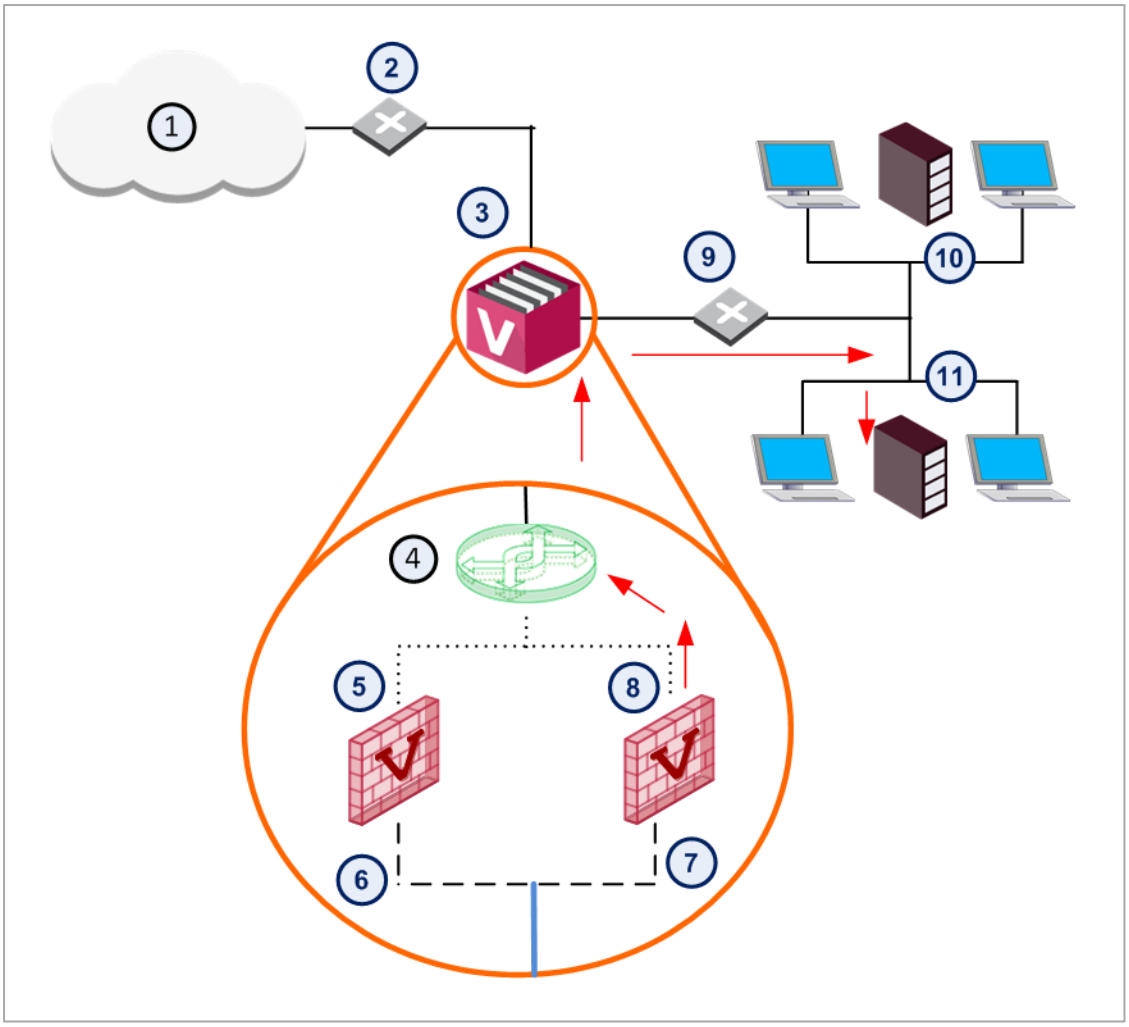
- Virtual System directly connected to a physical or VLAN interface
- Virtual System connected through a Virtual Switch
- Virtual System connected through a Virtual Router

  Note - Security Groups in Maestro and Scalable Chassis do not support Virtual Routers (Known Limitation 01413513).

Direct Connection to a Physical Interface

When traffic arrives at an interface (either physical or VLAN) that directly connects to a Virtual System, the connection itself determines the context and traffic passes directly to the appropriate Virtual System via that interface.

This diagram shows traffic from a physical VLAN switch that is sent to an interface on the VSX Gateway.



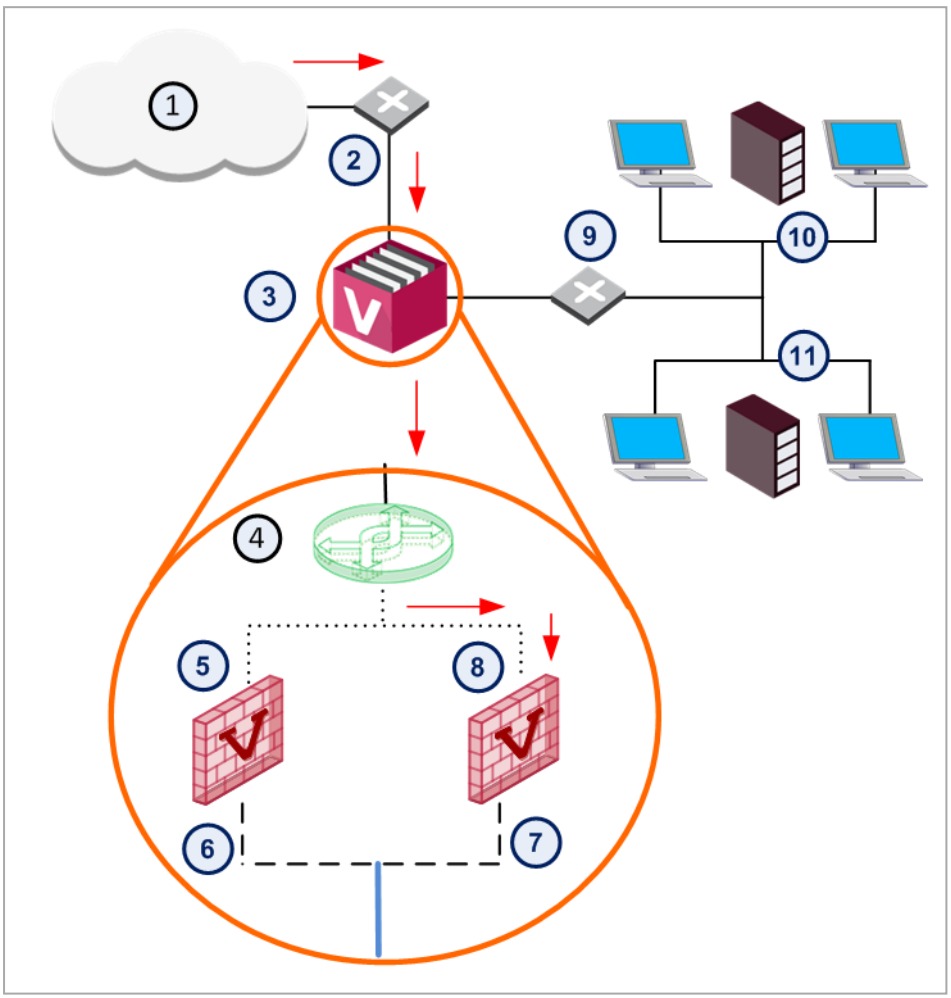
Item	Description		Item	Description
1	Internet		8	Virtual System 2
2	Router		9	VLAN Switch
3	VSX Gateway		10	VLAN 100
4	Virtual Switch		11	VLAN 200
5	Virtual System 1		-----	VLAN Interface
6	eth1.100		———	VLAN Trunk
7	eth1.200		.....	Warp Link

VSX automatically directs traffic arriving via VLAN Interface `eth1.200` to Virtual System 2 according to the context defined by the VLAN ID.

Connection through a Virtual Switch

Traffic arriving via a Virtual Switch passes to the appropriate Virtual System based on the destination MAC address, as defined in the Virtual Switch forwarding table.

Traffic arrives at the Virtual System via the Warp Link associated with the designated MAC address.



Item	Description		Item	Description
1	Internet		8	MAC 00:12:CI:Ce:00:03
2	Router		9	VLAN Switch
3	VSX Gateway		10	VLAN 100
4	Virtual Switch		11	VLAN 200
5	MAC 00:12:CI:Ce:00:01		-----	VLAN Interface
6	Virtual System 1		———	VLAN Trunk

Item	Description		Item	Description
7	Virtual System 2		.....	Warp Link

If the destination MAC address does not exist in the Virtual Switch forwarding table, the traffic is broadcast over all defined Warp Links.

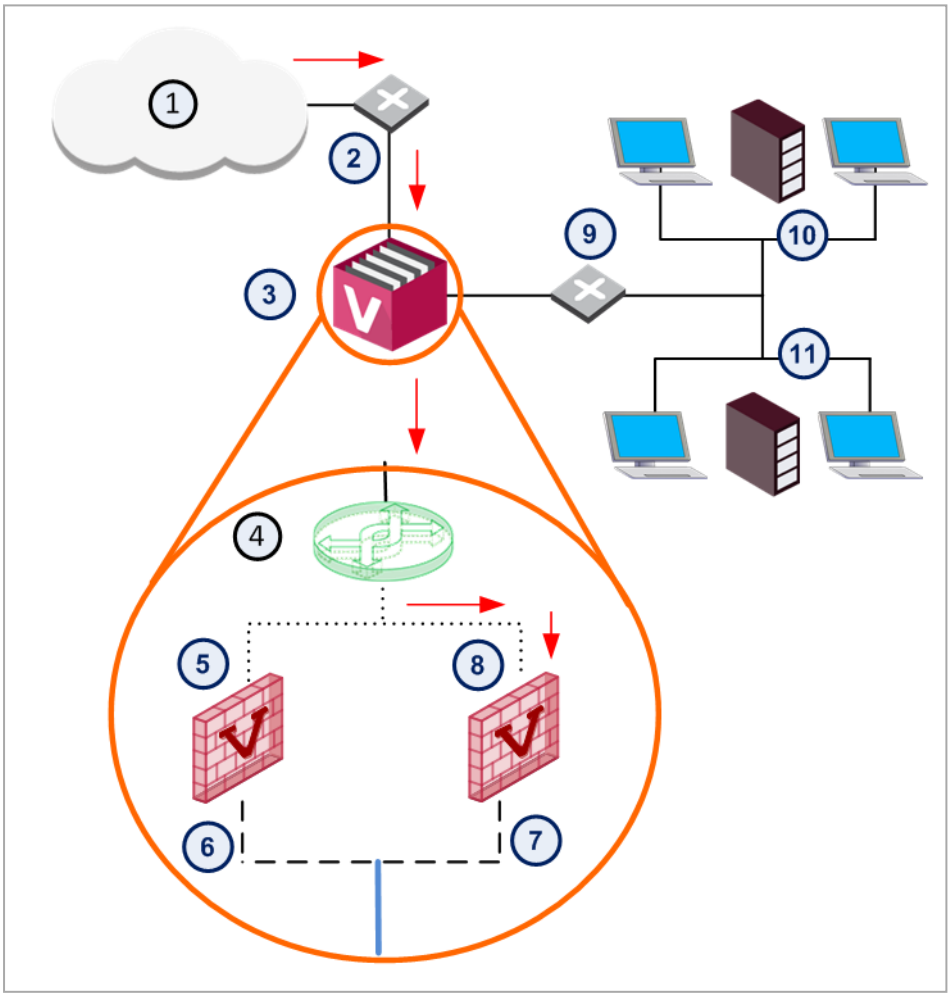
The Virtual Switch scenario is common for inbound traffic from external networks or the Internet.

Connection through a Virtual Router

Note - Security Groups in Maestro and Scalable Chassis do not support Virtual Routers (Known Limitation 01413513).

Traffic arriving via a Virtual Router passes to the appropriate Virtual System based on entries in the Virtual Router routing table.

Routing may be destination-based, source-based or both. Traffic arrives to the designated Virtual System via its Warp Link.



Item	Description		Item	Description
1	Internet		8	172.69.22.30
2	Router		9	VLAN Switch
3	VSX Gateway		10	VLAN 100
4	Virtual Router		11	VLAN 200
5	172.23.10.11		-----	VLAN Interface
6	Virtual System 1		———	VLAN Trunk
7	Virtual System 2		.....	Warp Link

Security Enforcement

Since each Virtual System functions as an independent Security Gateway, it maintains its own, unique security policy to protect the network behind it. The designated Virtual System inspects all traffic and allows or blocks it based on the rules contained in the security policy.

Forwarding to Destination

Each Virtual System maintains its own unique configuration and rules for processing and forwarding traffic to its final destination. This configuration also includes definitions and rules for NAT, VPN, and other advanced features.

VSX Routing Concepts

In This Section:

Routing Overview 70

Routing Between Virtual Systems 70

Route Propagation 72

Overlapping IP Address Space 73

More for Virtual Switch Route Propagation 74

NAT 74

Dynamic Routing 75

Note - Security Groups in Maestro and Scalable Chassis do not support Virtual Routers (Known Limitation 01413513).

Routing Overview

The traffic routing features in VSX network topologies are analogous to those available for physical networks.

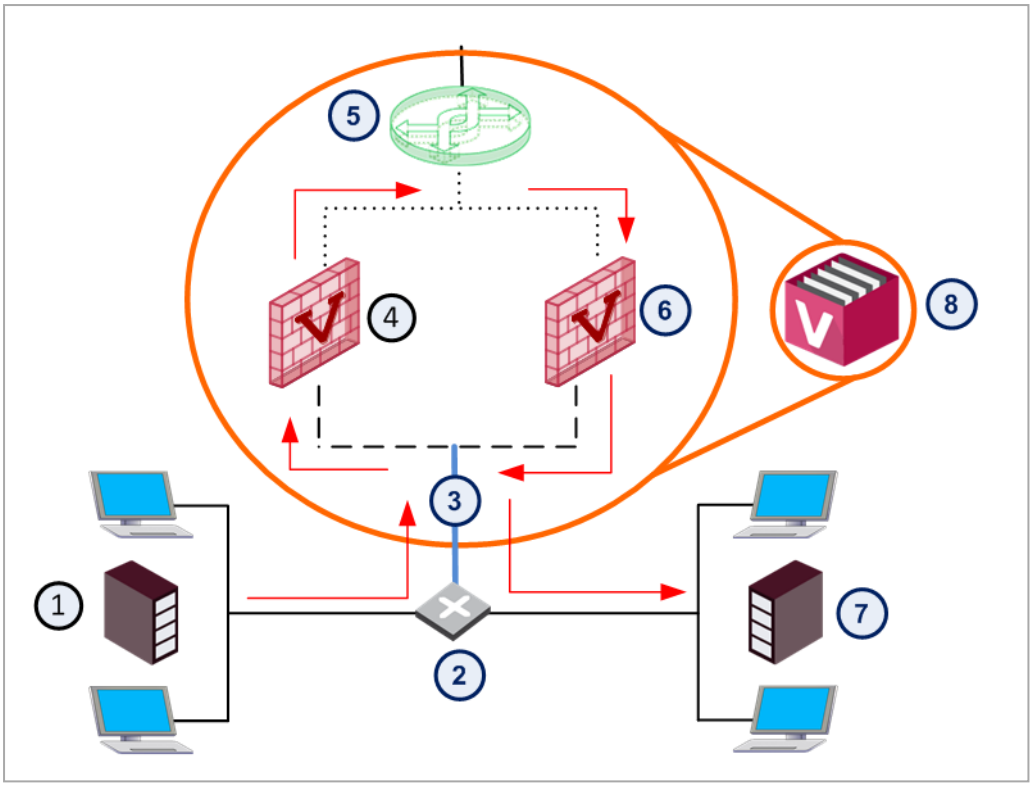
This section discusses several routing features and strategies as they apply to a VSX environment.

Routing Between Virtual Systems

Virtual Routers and Virtual Switches can be used to send traffic between networks located behind Virtual Systems, much in the same way as their physical counterparts.

The figure below shows an example of how Virtual Systems, connected to a Virtual Switch and a physical VLAN switch, communicate with each other.

In this example, a host in VLAN 100 sends data to a server located in VLAN 200.



Item	Description		Item	Description
1	VLAN 100		7	VLAN 200
2	VLAN Switch		8	VSX Gateway
3	VLAN Trunk		-----	VLAN Interface
4	Virtual System 1		———	VLAN Trunk
5	Virtual Switch		.....	Warp Link
6	Virtual System 2			

1. Traffic from the VLAN 100 host arrives at the VLAN switch, which inserts a VLAN tag and sends it to the VSX Gateway by way of a VLAN trunk.
2. Based on its VLAN tag, the VSX Gateway assigns the traffic to the Virtual System named VS1.
3. VS1 inspects the traffic according to its security policy and sends the traffic on to the Virtual Switch.

   Based on its routing configuration, VS1 sends the traffic to VS2 by way of the Virtual Switch.
4. VS2 inspects the traffic according to its security policy, inserts a VLAN tag, and sends it to back the VLAN switch.
5. The VLAN switch sends the traffic to the server located on VLAN 200.

Route Propagation

When a Virtual System is connected to a Virtual Router or to a Virtual Switch, you can choose to **propagate** its static routes to adjacent Virtual Devices.

This feature enables network nodes located behind neighboring Virtual Systems to communicate without the need for manual configuration of static routes.

Route propagation works by automatically updating Virtual Device routing tables with static routes that lead to the corresponding Virtual Systems.

Note - Route Propagation supports only static routes that you configure in SmartConsole in the Virtual System objects.
To use dynamic routes, you must configure the required dynamic settings in each required Virtual System on the VSX Gateway / each VSX Cluster Member.

Route Propagation using a Virtual Router

When Virtual Systems are connected to a Virtual Router, VSX propagates routes by automatically adding entries to the routing table contained in the Virtual Router.

Each entry contains a route pointing to the destination subnet using the Virtual System router-side Warp Interface (`wrpj`) as the next hop.

Route Propagation using a Virtual Switch

When Virtual Systems are connected to a Virtual Switch, VSX propagates routes by automatically adding entries to the routing table in each Virtual System.

Each entry contains a route pointing to the destination subnet using the Virtual System Warp Interface (`wrp`) IP address.

Overlapping IP Address Space

VSX facilitates connectivity when multiple network segments share the same IP address range (**IP address space**).

This scenario occurs when a single VSX Gateway protects several independent networks that assign IP addresses to endpoints from the same pool of IP addresses.

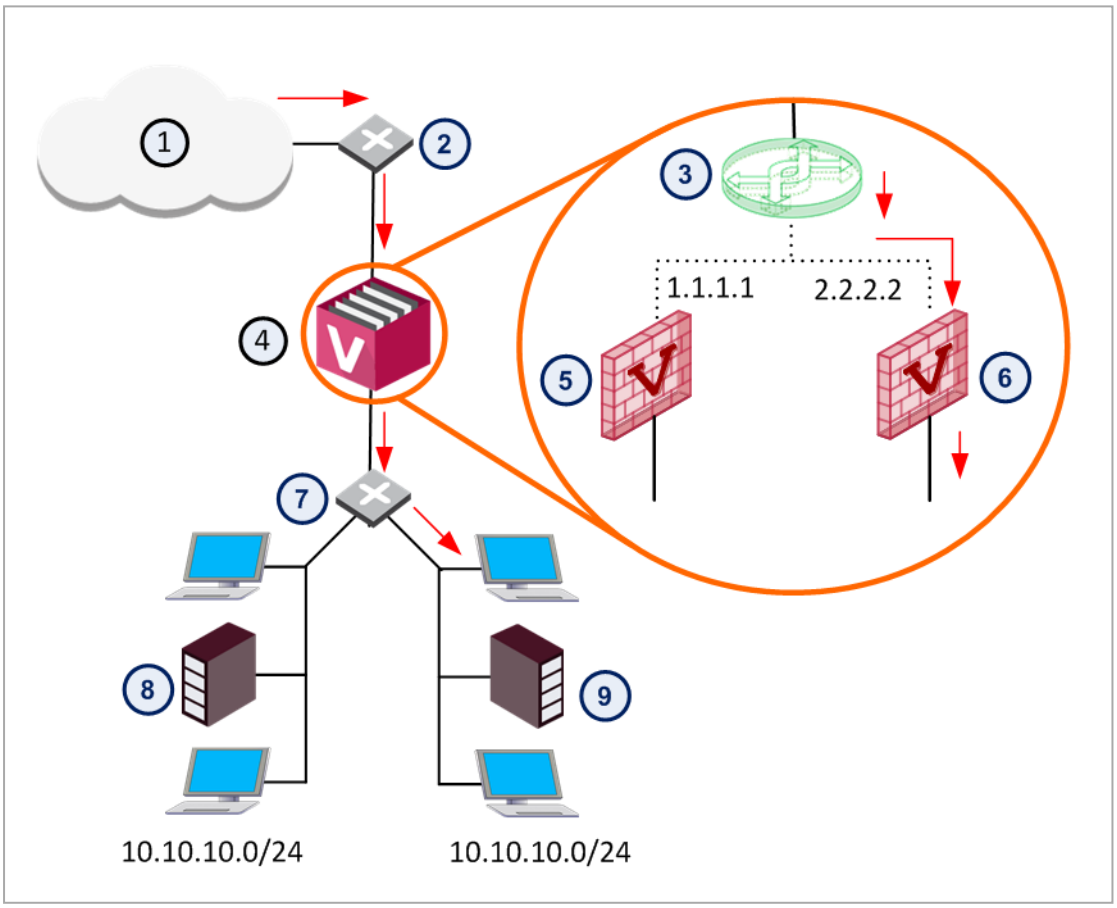
Thus, it is feasible that more than one endpoint in a VSX environment will have the identical IP address, provided that each is located behind different Virtual System.

Overlapping IP address space in VSX environments is possible because each Virtual System maintains its own unique state and routing tables.

These tables can contain identical entries, but within different, segregated contexts.

Virtual Systems use NAT to facilitate mapping internal IP addresses to one or more external IP addresses.

The below figure demonstrates how traffic passes from the Internet to an internal network with overlapping IP address ranges, using NAT at each Virtual System.



Item	Description		Item	Description
1	Internet		6	Virtual System 2

Item	Description		Item	Description
2	Router		7	Switch
3	Virtual Switch		8	Network 1
4	VSX Gateway		9	Network 2
5	Virtual System 1		.....	Warp Link

In this case, Network 1 and Network 2 share the same network address pool, which might result in identical overlapping IP addresses.

To prevent this, packets originating from or targeted to these networks are processed by their respective Virtual System using NAT to translate the original/overlapping addresses to unique routable addresses.

More for Virtual Switch Route Propagation

You are not required to manually define the topology, because this is done automatically.

But there are required manual steps in the VSX objects.

To update the topology map for each Virtual System after you enable route propagation:

1. For each Virtual System object that is connected to the Virtual Switch:
    a. Edit the object properties.

       Make sure Anti-Spoofing and VPN features are set correctly.
    b. Save the object.
2. Install the security policy for the affected Virtual Systems.

NAT

Virtual Systems support Network Address Translation (NAT), much in the same manner as a physical Security Gateway.

When a Virtual System, using either Static or Hide NAT, connects to a Virtual Router, you must propagate the affected routes to the Virtual Router.

To do so, you need to first define NAT addresses for Virtual Systems connected to a Virtual Router.

Dynamic Routing

The Virtual Devices can communicate and distribute routes using dynamic routing.

Each Virtual Device has its own routing daemon.

Virtual Systems support:

- OSPF
- RIP
- BGP
- PIM

Virtual Routers support:

- OSPF

VSX Clusters

A VSX Cluster has two or more identical, interconnected VSX Gateways for continuous data synchronization and transparent failover.

Virtual System Load Sharing (VSLS) enhances throughput by distributing Virtual Systems, with their traffic load, among multiple, redundant machines.

For more about Check Point ClusterXL features and functionality see the *R82 ClusterXL Administration Guide*.

High Availability

VSX supports High Availability and transparent failover for VSX Gateways and for Virtual Systems.

If the Active VSX Cluster Member fails, all sessions continue to run, securely and without interruption, on a Standby VSX Cluster Member.

Users stay connected and do not notice the failover. They are not required to authenticate again on failover.

Use Selective Sync to activate, delay, or disable VSX Cluster Member synchronization.

Virtual System Load Sharing (VSLS)

Load Sharing offers significant performance advantages while providing failover for individual Virtual Systems.

Using multiple Gateways instead of a single gateway significantly increases performance for CPU intensive applications such as VPNs, Security Servers, Policy Servers, and Active Directory (LDAP).

By distributing Virtual System instances between different VSX Cluster Members, the performance load is efficiently spread amongst the VSX Cluster Members.

For example, Active Virtual System 1 runs on VSX Cluster Member A, while Active Virtual System 2 runs on VSX Cluster Member B.

Standby and Backup Virtual System instances are likewise distributed amongst VSX Cluster Members to maximize throughput, even in a failover scenario.

VSLS provides an excellent scalability solution, allowing administrators to add additional VSX Cluster Members to an existing VSLS cluster as traffic loads and performance requirements increase.

Getting Started with VSX

Workflow

1. Plan the complete VSX topology before you start the installation and configuration, because it is not possible to change some settings after you configure them.

   Important - If you use a Multi-Domain Security Management Server, plan which Domain Management Server would manage the VSX Gateway / VSX Cluster and which Domain Management Servers would manage the VSX Virtual Systems, VSX Virtual Routers, and VSX Virtual Switches. See *"Using VSX with Multi-Domain Server" on page 180*.

   - Use a VSX Gateway or a VSX Cluster?
   - Use VSX Virtual Routers?

     See *"Virtual Devices" on page 51*.

2. Install the applicable Management Server.

   See the *Installation and Upgrade Guide* for your version.

3. Install a VSX Gateway or VSX Cluster Members.

   See the *Installation and Upgrade Guide* for your version.

4. In SmartConsole, configure the object for the VSX Gateway or the VSX Cluster.

   See:

   - *"Configuring VSX Gateways" on page 98*
   - *"Configuring VSX Clusters" on page 185*

5. In SmartConsole, configure the objects for the VSX Virtual Routers, if you decided to use them.

   See *"Working with Virtual Routers" on page 132*.

6. In SmartConsole, create the objects for the VSX Virtual Switches, if you decided to use them.

   See *"Working with Virtual Switches" on page 128*

7. In SmartConsole, create the objects for the VSX Virtual Systems.

   See *"Working with Virtual Systems" on page 109*.

8. In SmartConsole, configure the objects for the VSX Virtual Systems.

   Enable and configure the applicable Software Blades.

See the *Security Gateway Guide* for your version.

9. In SmartConsole, configure the applicable Access Control Policies and install them on the Virtual Systems.
10. In SmartConsole, configure the applicable Threat Prevention Policies and install them on the Virtual Systems.
11. In SmartConsole or SmartView, examine the logs from the Virtual Systems.

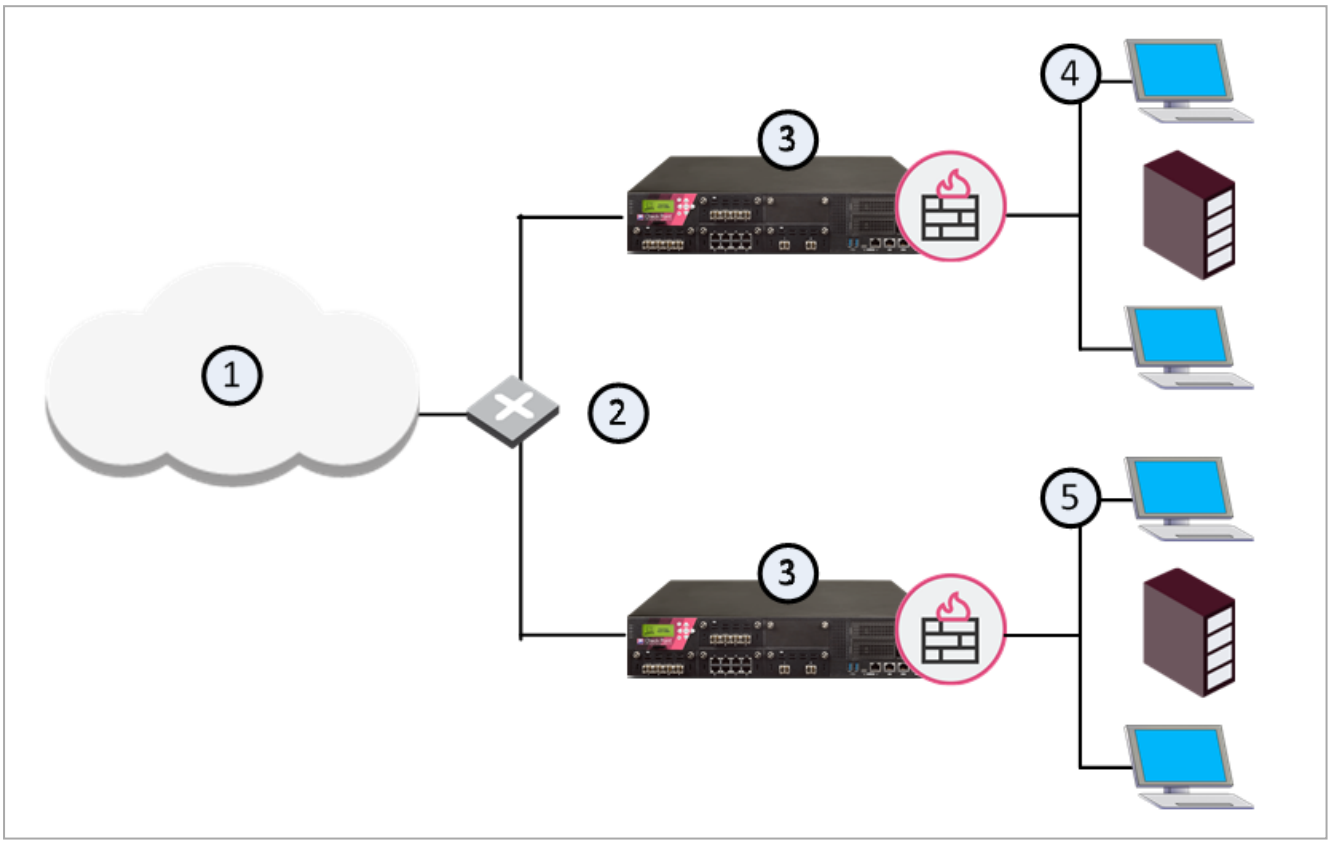
Deploying VSX - Internal Network Deployment Strategies

In This Section:

Security Gateway Deployment on a Physical Network 80
VSX Virtual System Deployment Strategies 81
Physical Internal Interface for Each Virtual System 81
Virtual Systems with Internal VLAN Interfaces 82
Internal Virtual Router with Source-Based Routing 84
Virtual Systems in Bridge Mode 85

Security Gateway Deployment on a Physical Network

In large physical network deployments, multiple Check Point security products, such as Security Gateways, are deployed to protect network segments.



Item	Description
1	Internet
2	Router
3	Security Gateways
4	Network 1
5	Network 2

Each Security Gateway physically connects to its own internal protected network and to a router for access to other internal networks and the Internet.

VSX Virtual System Deployment Strategies

In a VSX environment, Virtual Systems protect internal networks.

This section shows sample VSX deployments with Virtual Systems to protect internal networks.

Each example highlights different VSX features.

In a real-world deployment, you can combine features to create a powerful cyber security solution for complex enterprise environments.

Physical Internal Interface for Each Virtual System

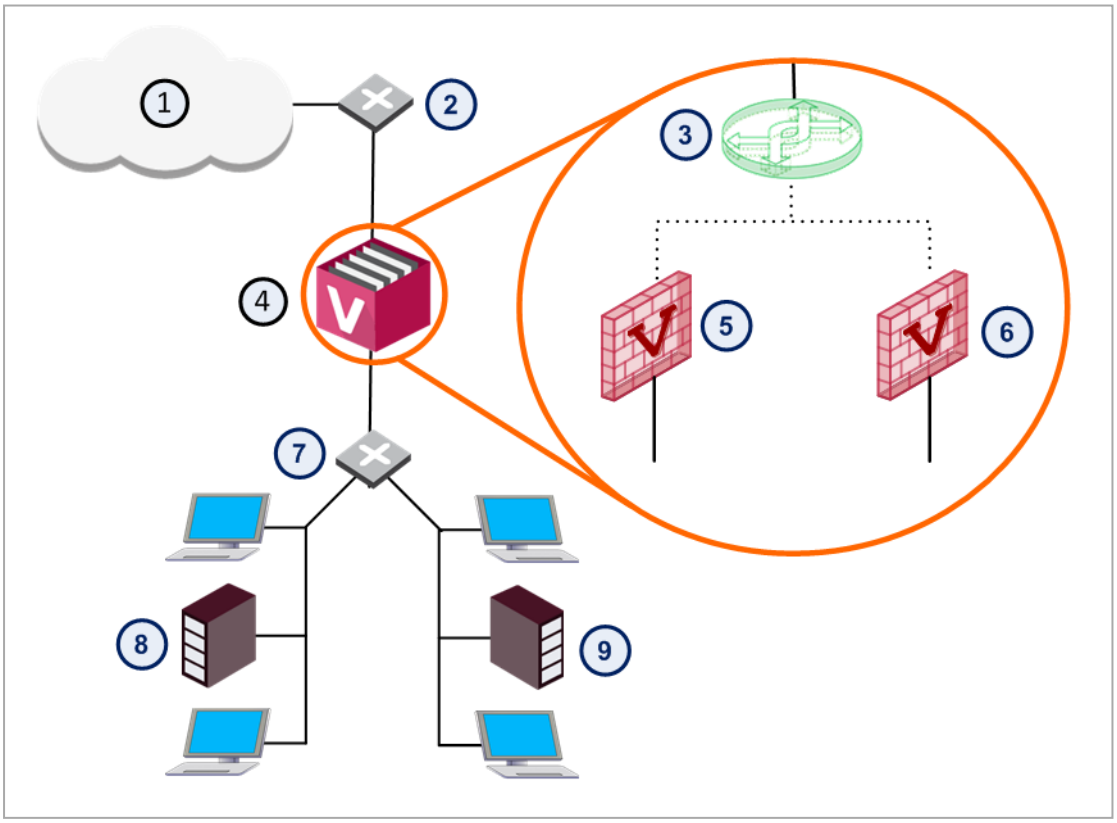
In a basic VSX configuration, Virtual Systems connect directly to protected internal networks through physical interfaces on the VSX Gateway.

A Virtual Switch connects between internal networks, and to the Internet.

This deployment is suitable for protecting a small, fixed quantity of internal networks.

The main disadvantage of this deployment is that each protected network requires its own dedicated physical interface on the VSX Gateway.

Obviously, this deployment is not suitable for networks that require many Virtual Systems.



Item	Description		Item	Description
1	Internet		6	Virtual System 2
2	Router		7	Switch
3	Virtual Switch		8	Network 1
4	VSX Gateway		9	Network 2
5	Virtual System 1		.....	Warp Link

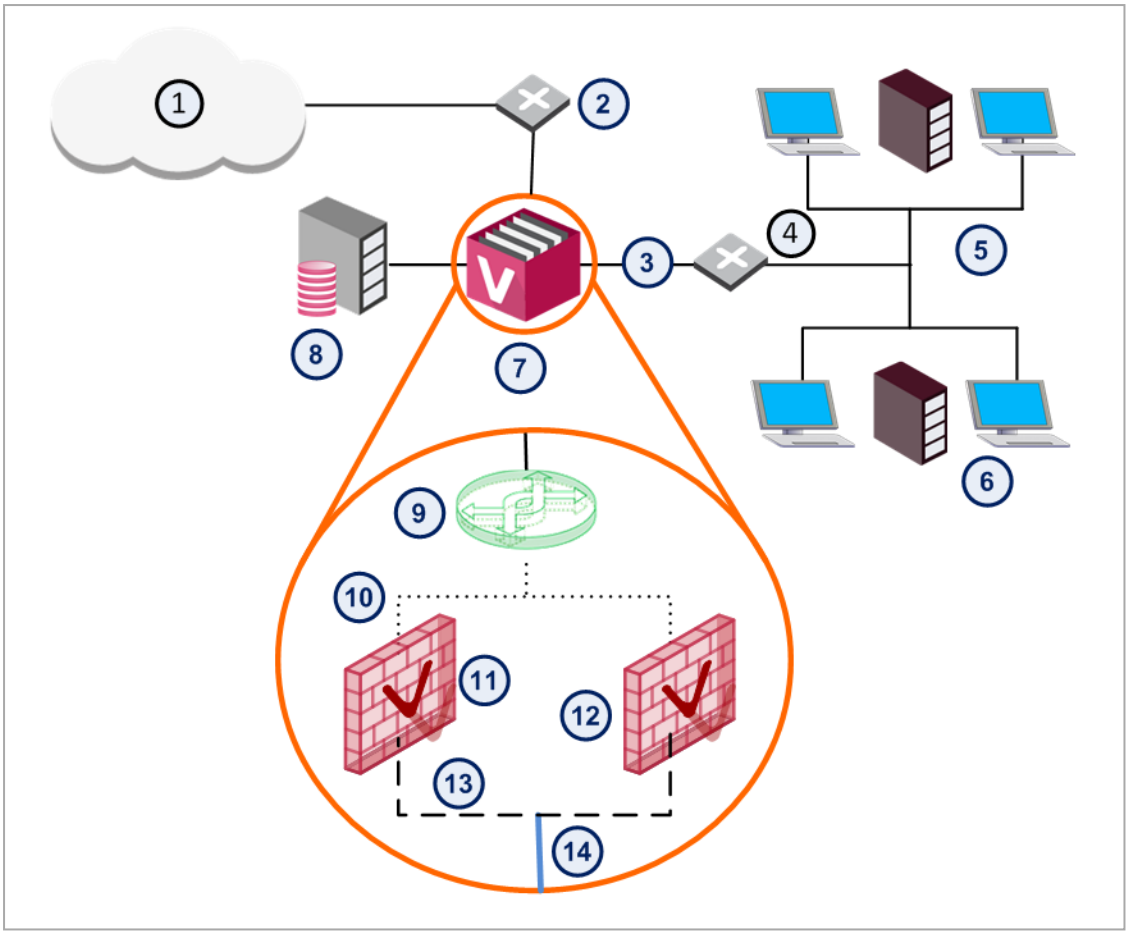
Virtual Systems with Internal VLAN Interfaces

In this deployment example, Virtual Systems connect to internal protected networks through VLAN interfaces.

The VSX Gateway connects to a VLAN switch with an 802.1q VLAN trunk, which is an aggregate of all VLANs passing through it.

This deployment option is appropriate for environments where many Virtual Systems protect many internal networks with one VSX Gateway or cluster.

VLANs provide scalability and granularity, to provision more Virtual Systems and protected networks quickly, without changing the existing IP address structure.



Item	Description		Item	Description
1	Internet		8	Management Server
2	Router		9	Virtual Switch
3	Physical interface		10	Warp interface
4	VLAN Switch		11	Virtual System 1
5	Network 1		12	Virtual System 2
6	Network 2		13	VLAN Interface
7	VSX Gateway		14	VLAN Trunk

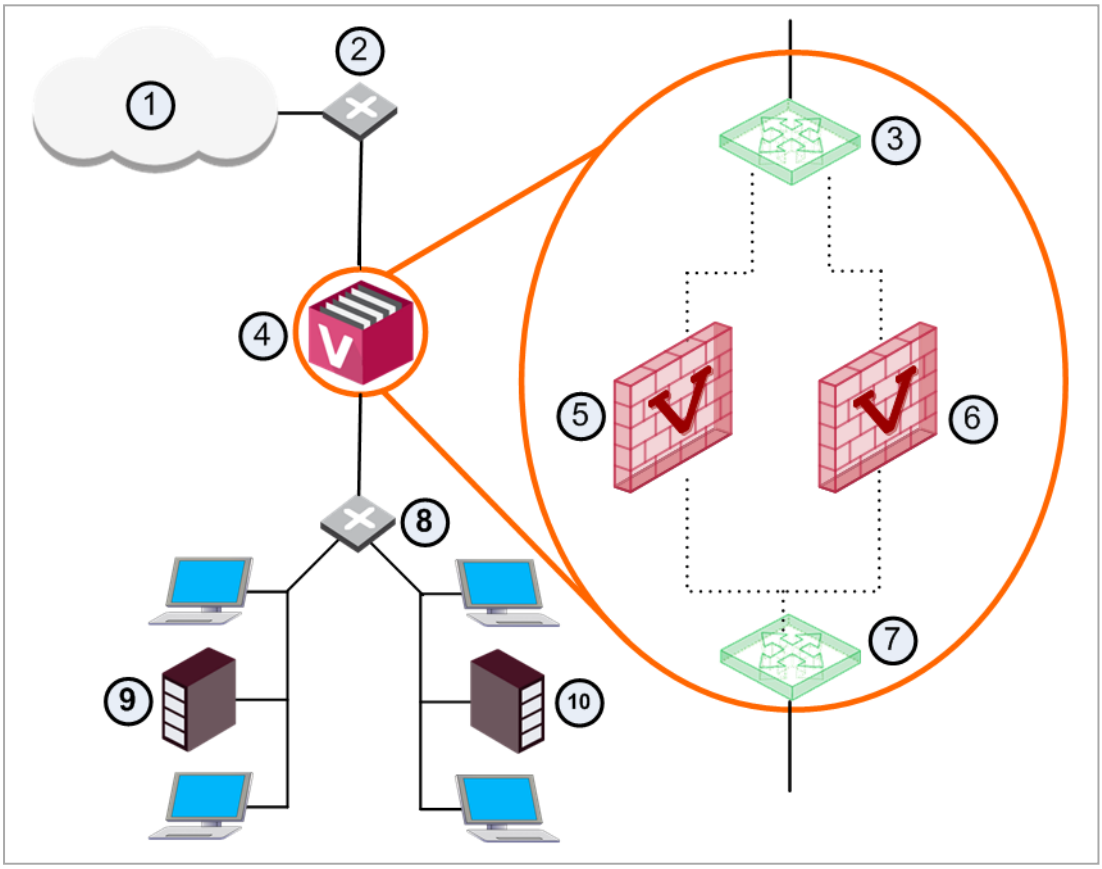
Internal Virtual Router with Source-Based Routing

Note - Security Groups in Maestro and Scalable Chassis do not support Virtual Routers (Known Limitation 01413513).

This deployment scenario enables Virtual Systems to connect to protected networks using a single physical interface without VLAN technology.

The Virtual Router uses source-based routing rules to forward traffic to the appropriate Virtual System based on its source IP address.

In a VSX deployment with each Virtual System connected to a single Virtual Router: You can configure the Virtual Router to use source-based routing rules, to forward traffic to the appropriate Virtual System, based on the source IP address.



Item	Description		Item	Description
1	Internet		7	Virtual Router
2	Router		8	Router
3	Virtual Switch		9	Network 1

Item	Description		Item	Description
4	VSX Gateway		10	Network 2
5	VS 1		.....	Warp link
6	VS 2			

Notes for this scenario:

- Each Virtual System uses a public IP address to connect to the Virtual Switch.
- Each local network connected to a Virtual Router uses private IP addresses.
- This deployment does not support overlapping IP addresses.
- Anti-Spoofing protection does function for packets originating from the shared internal interface.

  We recommend that you configure the internal physical router to perform Anti-Spoofing protection.

Virtual Systems in Bridge Mode

A Virtual System in bridge mode implements native Layer 2 bridging instead of IP routing and can co-exist with Layer 3 Virtual Systems on the same VSX Gateway.

This allows network administrators to easily and transparently deploy a Virtual System in an existing network topology without reconfiguring the existing IP routing scheme.

Bridge Mode deployments are particularly suitable for large-scale clustered environments.

See *"Bridge Mode" on page 270*.

Deploying VSX - Organizational Deployment Strategies

In This Section:

Enterprise Deployments 86
Managed Service Providers Using Multi-Domain Server 91
Data Centers 93

Note - Security Groups in Maestro and Scalable Chassis do not support Virtual Routers (Known Limitation 01413513).

This section presents deployment scenarios for different types of large organizations and illustrates how VSX provides security both internally and at the perimeter.

The discussion covers the following types of organizations:

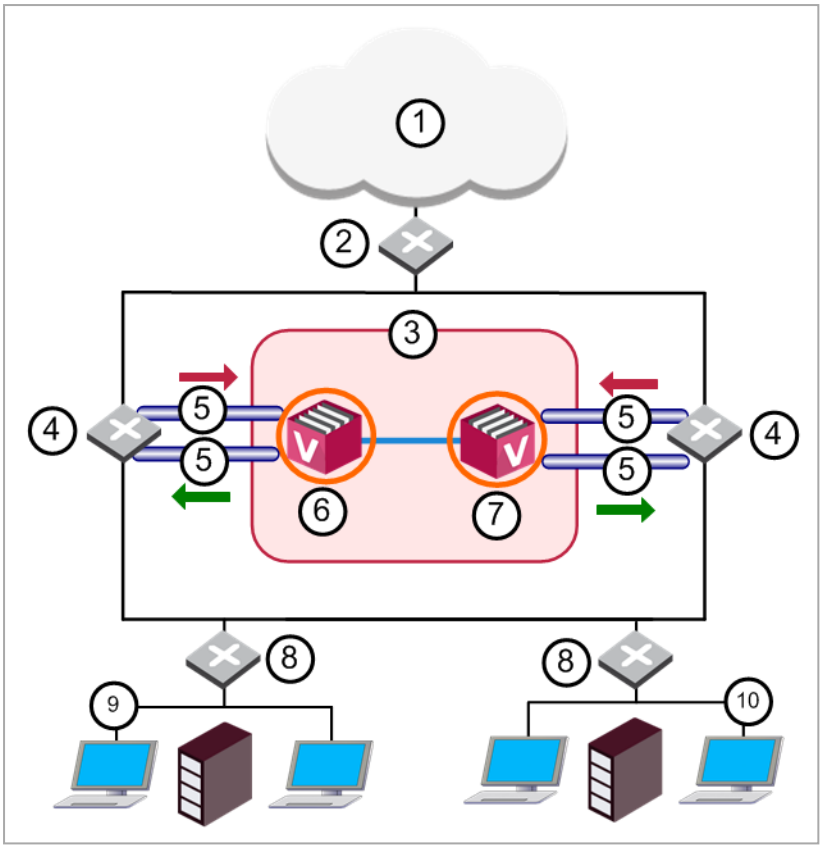
- Large Enterprises
- Managed Service Providers
- Data Centers

Enterprise Deployments

Large enterprise network environments typically have a variety of diverse networks, distributed over multiple locations around the world. These networks often have different security and access requirements for various departments and branches. The ability to centrally manage cyber security, and to maintain throughput, is a critical requirement.

Core Network Security

Many Enterprise environments are based on core networks. Situated adjacent to core network backbone switches, VSX protects the internal network by providing security at Layer 2, Layer 3 or both. VSX communicates with the core network using the existing infrastructure. With Virtual Systems in the Bridge Mode, VSX can protect departmental networks, while simultaneously preventing network segmentation. In this case, switches are located at the entrance to each department's network.



Item	Description		Item	Description
1	Internet		8	LAN Switches
2	Core Network Backbone switch		9	Sales
3	VSX Cluster		10	Finance
4	Router			Sync Network
5	VLAN			Physical Interface
6	Member 1			VLAN Trunk
7	Member 2			

VSX ensures connectivity between the core network and the Internet or external networks, while providing perimeter security.

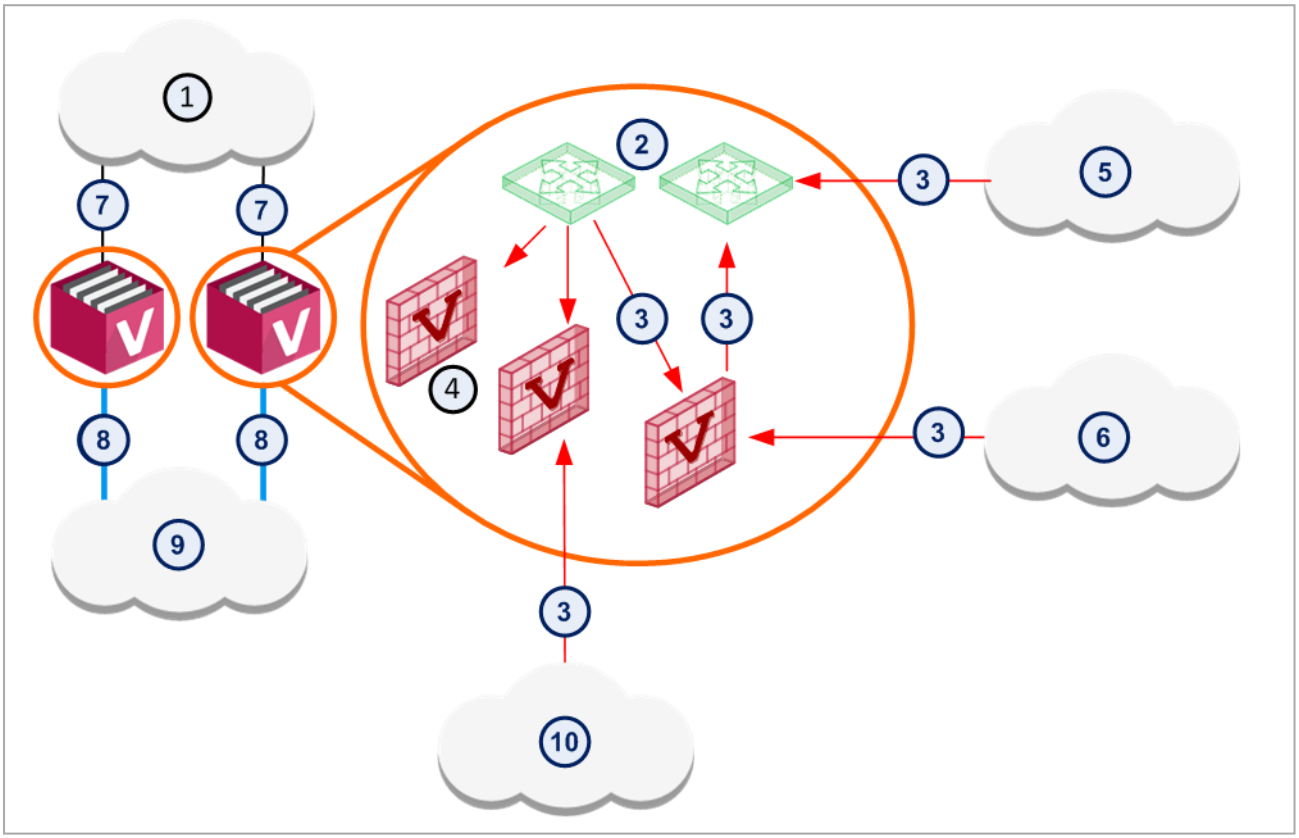
Security can be configured on a per VLAN basis.

Dynamic Routing

In an enterprise network with dynamic routing protocols (OSPF/BGP), VSX secures the DMZ services, VPN peers, Domains and partner networks.

In this example, BGP neighbor updates in the routed core network are selectively redistributed to application networks.

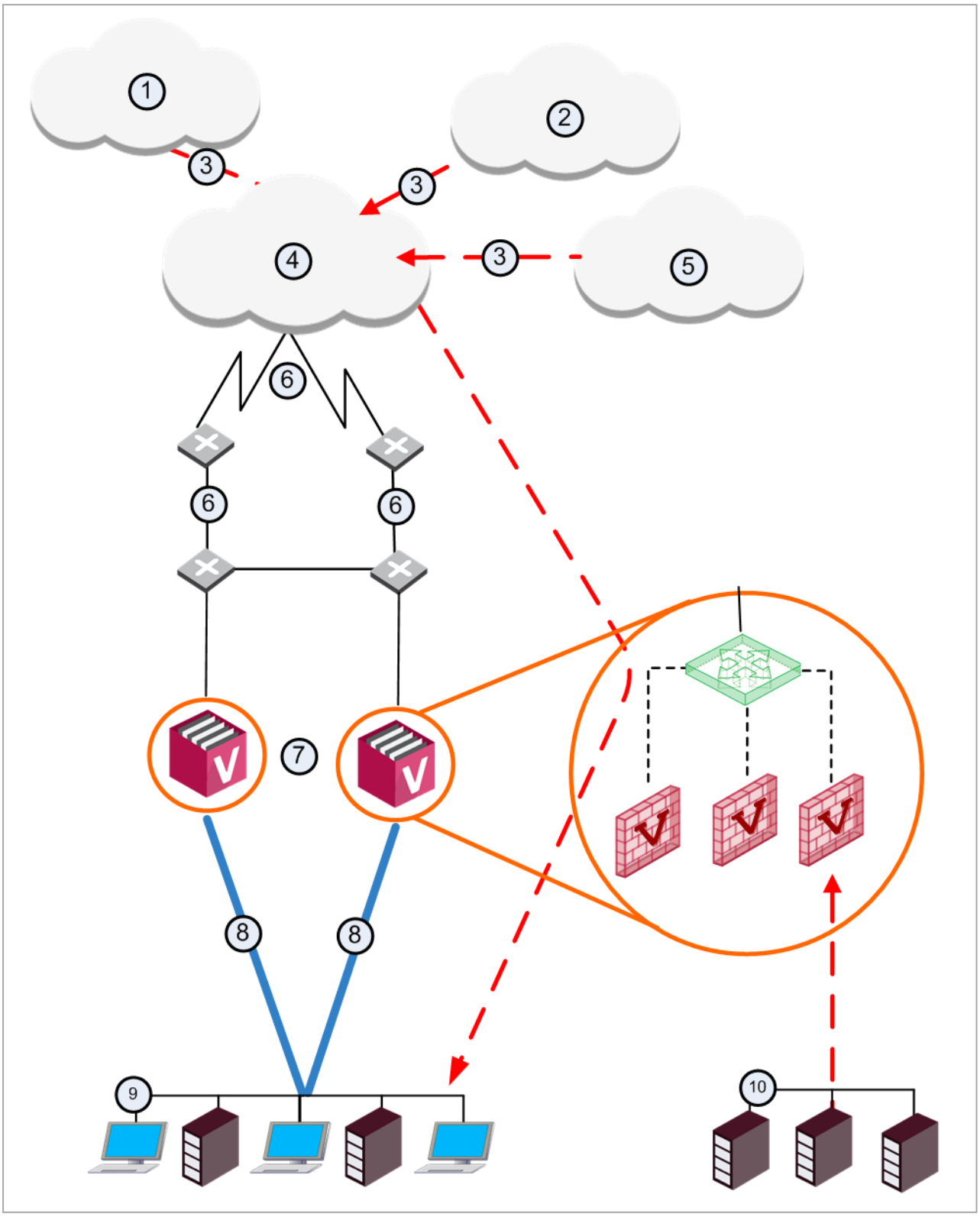
OSPF provides connectivity between Virtual Routers, Virtual Systems, the core network and application networks.



Item	Description		Item	Description
1	Internet		6	Partner Network
2	Virtual Routers		7	BGP
3	OSPF		8	OSPF 802.1q
4	Virtual Systems		9	BGP in Routed Core
5	Extranet		10	DMZ

Perimeter Security

For example, security is enforced on each VLAN. The OSPF and BGP Dynamic routing protocols provide connectivity to multiple security zones along the perimeter.



Item	Description		Item	Description
1	Partner Access		6	BGP
2	Customers		7	VSX Cluster
3	IPsec tunnel		8	802.1q VLAN Trunk
4	Internet		9	Internal Network
5	Partner		10	DMZ

Notes to this scenario:

- Partners access network resources remotely via Virtual Systems
- Each Virtual System has its own security policy based on its requirements
- Logs and audit information for each partner are collected separately, and saved to a private database
- Applications and services are segregated by private Virtual Systems
- Multiple Virtual Routers / Virtual Switches are used to control the access paths

Managed Service Providers Using Multi-Domain Server

Managed service providers give connectivity and security services for Domain networks.

Some of these Domains require remote access capabilities.

In this service oriented environment, VSX and Multi-Domain Server provide central management and make connectivity and security easier, without affecting the existing IP topology.

In this scenario, a VSX Cluster is in a Point of Presence (POP) deployment for a service provider.

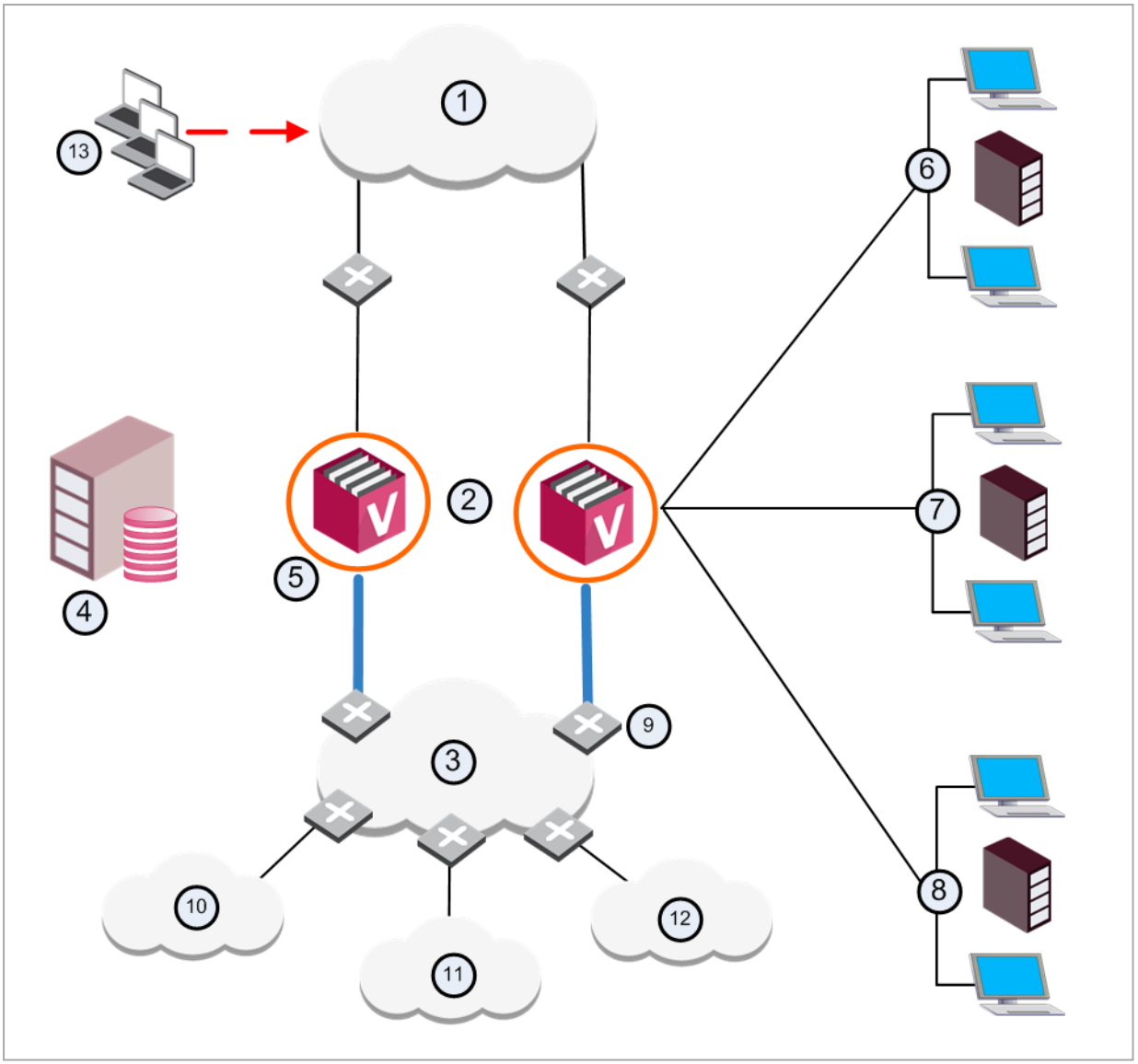
VSX consolidates hardware for the service provider and ensures privacy and secure connectivity solutions (VPN) for users.

This scenario is appropriate for High Availability and Virtual System Load Sharing cluster modes.

VSX and Multi-Domain Server provide a centralized, granular provisioning system for a number of Domains.

Applications and services are separated by discrete Virtual Systems.

Access to these services and applications is based on need.



Item	Description
1	Internet. Routers are between the VSX Cluster Members and the Internet.
2	VSX Cluster. One VSX Cluster Member handles the Local Exchange, and another VSX Cluster Member handles server traffic of different Domains.
3	Core IP VPN Network.
4	Multi-Domain Server at the Network Operation Center monitors POP and connects to VSX Gateway. The Multi-Domain Log Server in the NOC collects data for each Domain and stores the logs in separate private databases.
5	Multi-Domain Server at the NOC and the VSX Gateway make the Local Exchange.

Item	Description
6	Domain A web servers.
7	Domain B DMZ.
8	Domain C mail servers.
9	PE Router.
10, 11, 12	Domain A, B, and C. Each Domain manages its own security and cannot define Virtual Systems or other network components. Domains have secure VPN connectivity.
13	Remote access

Data Centers

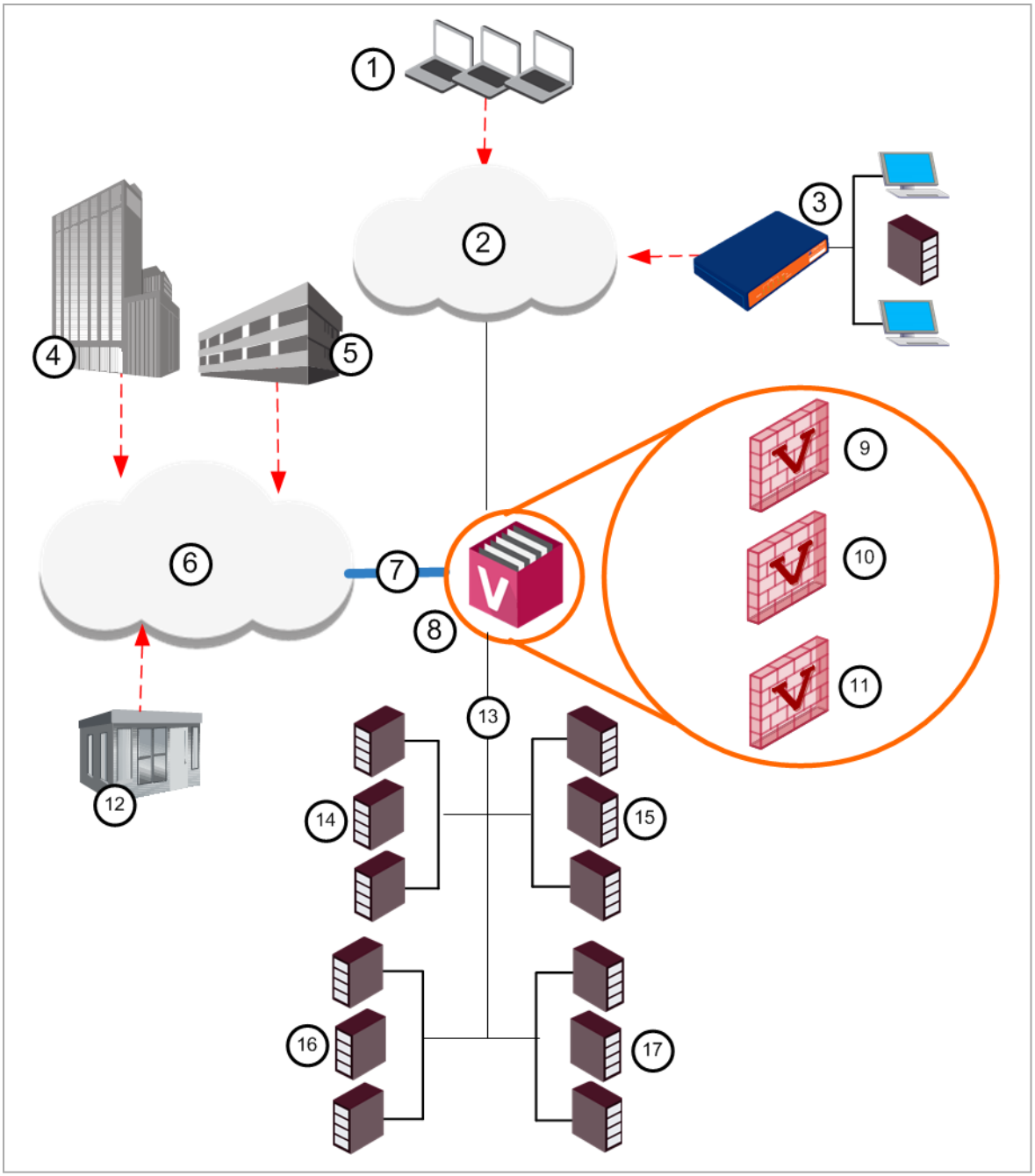
Data center providers supply external hosting services for Domain servers and databases.

The service typically includes infrastructure, connectivity, and security for multiple Domains.

For example, you can have a scenario such as:

- Multiple Domain networks sharing a common physical infrastructure.
- Backbone that provides connectivity between each Domain and the data center.
- Domain A connects to its web hosting servers.
- Domain B connects to its mail servers.
- Domain C connects to its database servers.

For cyber security and management, the data center provider deploys a VSX Gateway with one Virtual System for each Domain.



Item	Description		Item	Description
1	Remote Users		10	Virtual System for Customer A
2	Internet		11	Virtual System for Customer C
3	Remote network behind VPN-1 Edge		12	Customer C
4	Customer B		13	Data Center

Item	Description		Item	Description
5	Customer A		14	Customer A web servers each with separate VLAN ID
6	MPLS Backbone		15	Customer B mail servers
7	802.1q		16	Customer A Extranet
8	VSX Gateway		17	Customer C databases
9	Virtual System for Customer A			

This scenario offers a cost effective scalability solution for network expansion by means of remote connectivity.

In this example, a VPN connection between a Domain Virtual System and a Check Point appliance that protects a remote network, integrates that network in the MPLS core.

A Virtual System can give access to remote users who connect intermittently.

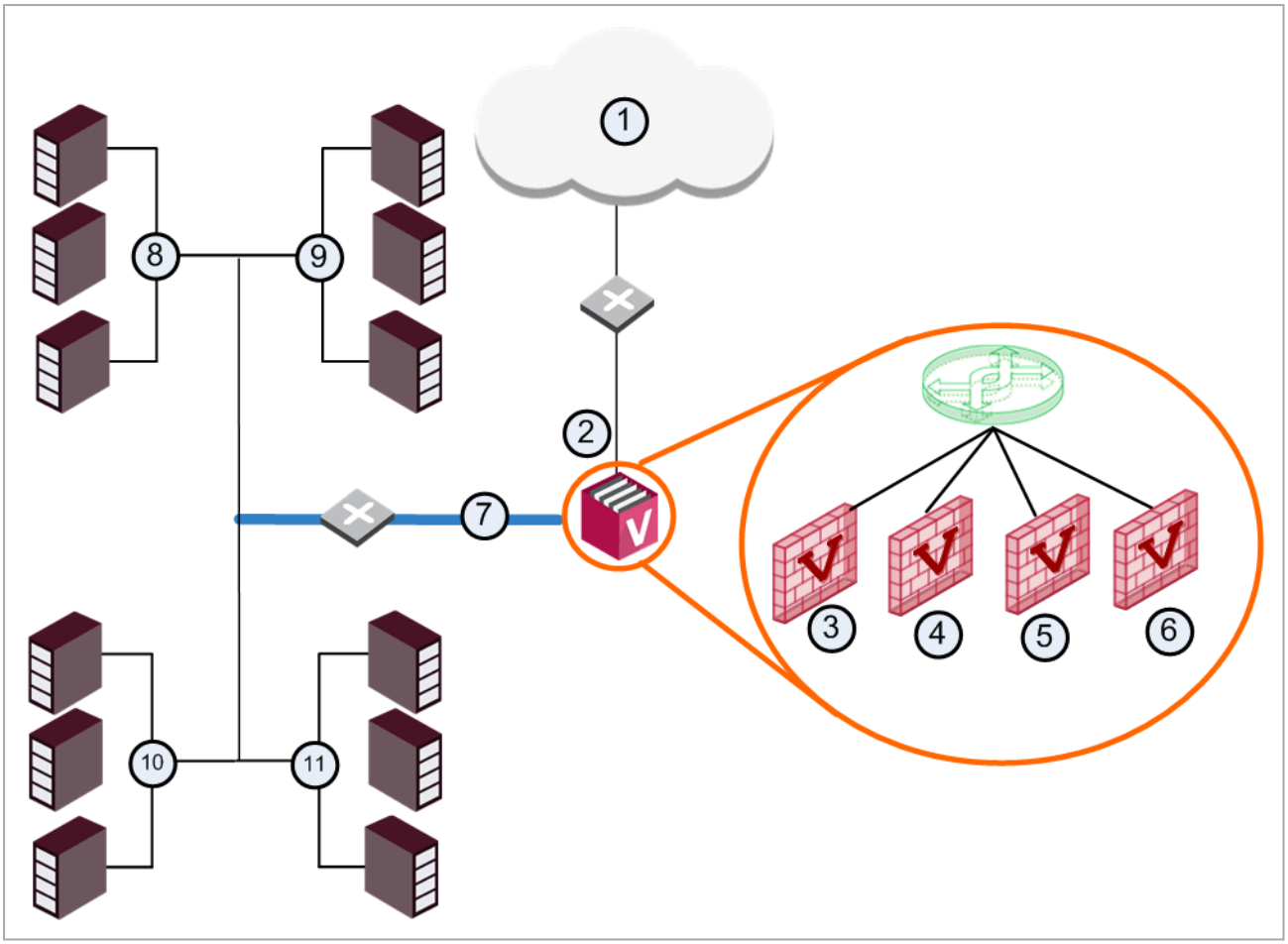
Data Centers in an Enterprise

This example scenario illustrates how VSX provides security management for enterprise data centers.

By assigning Layer 2 connections to Virtual Systems, VSX reduces the number of physically managed devices within a data center while providing the same high level of security.

For example, a VSX Gateway allows authorized users to access data center resources.

The objective here is to protect shared resources with differing access permissions and security requirements, while implementing network granularity.



Item	Description		Item	Description
1	Internet		7	VLAN Trunk
2	VSX Gateway		8	Web Servers VLAN 02
3	VLAN 02		9	Data Bases VLAN 03
4	VLAN 03		10	Application A VLAN 04
5	VLAN 04		11	Application B VLAN 05
6	VLAN 05			

For example, one Virtual System protects databases against SQL vulnerabilities.

Another Virtual System protects Web Servers using IPS.

When new applications and services are added to the enterprise data center, new Virtual Systems are easily created to secure them according to their specific requirements.

Configuring VSX

Overview

This chapter explains how to use SmartConsole provision, configure and manage Virtual Devices in a VSX environment.

If you define or configure VSX objects in a Multi-Domain Server deployment: connect with SmartConsole to the Domain Management Server that manages the Virtual Devices. For procedures, see *"Using VSX with Multi-Domain Server" on page 180*.

To configure Virtual Devices, make sure:

- The Management Servers (Security Management Server or Multi-Domain Server) are configured and running.
- SmartConsole is installed on the appropriate computer.

This chapter assumes that you are familiar with SmartConsole and how to configure standard Security Gateway objects and Security Policies.

Many Virtual Device and policy operations are the same as physical Security Gateways and these standard procedures are not in this Administration Guide.

Rules and Security Policies

You use the same procedures to define and install Security Policies on a VSX Gateway or Virtual System as for a physical Security Gateway.

This statement also applies to the use of IPv6 in Security Policies. These procedures are not included in this Administration Guide.

Configuring VSX Gateways

In This Section:

Creating a New VSX Gateway *99*

Wizard Step 1: Defining VSX Gateway General Properties *99*

Wizard Step 2: Establishing SIC Trust *100*

Wizard Step 3: Defining Physical Interfaces *101*

Wizard Step 4: Virtual Network Device Configuration *102*

Wizard Step 5: VSX Gateway Management *103*

Completing the VSX Wizard *103*

Configuring the Security Policy *103*

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.
- Virtual Routers are not supported (Known Limitation 01413513).
- It is not supported to enable IPv6 in the Security Group before you create and configure a new VSX Gateway object in the Traditional VSX mode. You must first create the new VSX Gateway object and only then enable and configure IPv6 in Gaia gClish (Known Limitation 01341918).

Creating a New VSX Gateway

Notes:

- It is not supported to convert an existing Security Gateway to a VSX Gateway.
- It is not supported to convert an existing VSX Gateway to a Security Gateway.

This section explains how to create a new VSX Gateway using the **VSX Gateway Wizard**.

After you complete the VSX Gateway Wizard, you can change the VSX Gateway definition from SmartConsole.

For example, you can add or delete interfaces, or configure existing interfaces to support VLANs.

To start the VSX Gateway wizard:

1. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages the VSX Gateway.
2. From the left navigation panel, click **Gateways & Servers**.
3. At the top, click **New** > **VSX** > **Gateway**.

   The **General Properties** page of the **VSX Gateway Wizard** opens.

Wizard Step 1: Defining VSX Gateway General Properties

Configure these parameters on the **General Properties** page:

- **VSX Gateway Name**: Unique, alphanumeric name for the VSX Gateway. The name cannot contain spaces or special characters except the underscore.
- **VSX Gateway Addresses**: Management interface addresses.

  Note - If you define an IPv6 IP address you must also define an IPv4 address.

- **VSX Gateway Version**: Select the VSX version installed on the VSX Gateway from the drop-down list.

Wizard Step 2: Establishing SIC Trust

Initialize SIC trust between the VSX Gateway and the Management Server.

They cannot communicate without Trust.

Initializing SIC Trust

When you create a VSX Gateway, you must enter the same Activation Key you entered during the First Time Configuration Wizard.

Enter and confirm the activation key and then click **Initialize**.

If you enter the correct activation key, the **Trust State** changes to `Trust established`.

Troubleshooting SIC Trust Initialization Problems

If SIC trust was not successfully established, click **Check SIC Status** to see the reason for the failure.

The most common issues are an incorrect activation key and connectivity problems between the Management Server and the VSX Gateway.

Troubleshooting to resolve SIC initialization problems:

- Re-enter and re-confirm the activation key.
- Make sure that the IP address defined in **General Properties** is correct.
- Ping the Management Server to test the connectivity. Resolve connectivity issues.
- From the VSX Gateway command line, use the `cpconfig` command to re-initialize SIC.

  After this process completes, click **Reset** in the wizard and then re-enter the activation key.

For more about resolving SIC initialization, see the *R82 Security Management Administration Guide*.

Troubleshooting SIC in a Scalable Platform Security Group

Troubleshooting SIC Reset in Security Groups

Resetting SIC takes 3-5 minutes.

If resetting of the SIC was interrupted (for example, by loss of network connectivity), run the Expert mode command "`g_all cp_conf sic state`" on the Security Group to get the SIC state and follow these steps:

SIC state	Do this
`Trust established`	Repeat the SIC reset procedure.
`Initialized, but Trust was not established`	1. Reboot all Security Group Members. 2. In SmartConsole, open the Security Group object. 3. Go to **General Properties** page > **Communication**. 4. Initialize SIC. 5. Install the policy.

SIC Cleanup in Security Groups

To resolve other SIC issues, do a SIC cleanup in the Expert mode:

```
asg_blade_config reset_sic -reboot_all <activation_key>
```

Wizard Step 3: Defining Physical Interfaces

In the **VSX Gateway Interfaces** window, define physical interfaces as VLAN trunks.

The window shows the interfaces currently defined on the VSX Gateway.

To define an interface as a VLAN trunk, select **VLAN Trunk** for the interface.

Wizard Step 4: Virtual Network Device Configuration

Note - Configuration with a Non-Dedicated Management Interface (Non-DMI, shared interface) is deprecated and not supported.

If you chose the **Custom Configuration** option, the **Virtual Network Device Configuration** window opens.

In this window, define a Virtual Device with an interface shared with the VSX Gateway.

If you do not want to define a Virtual Device at this time, click **Next** to continue.

To define a Virtual Device with a shared interface:

1. Select **Create a Virtual Device**.
2. Select the **Virtual Network Device type** (**Virtual Router** or **Virtual Switch**).
3. Select the **Shared physical interface** to define a non-DMI VSX Gateway.

   Do not select the management interface if you want to define a **Dedicated Management Interface (DMI)** VSX Gateway.

   If you do not define a shared Virtual Device, a DMI VSX Gateway is created by default.

   Important - This setting cannot be changed after you complete the VSX Gateway Wizard. If you define a non-DMI VSX Gateway, you cannot change it to a DMI VSX Gateway later.
4. Define the **IP address** and **Net Mask** for a Virtual Router.

   These options are not available for a Virtual Switch.
5. **Optional:** Define a **Default Gateway** for a Virtual Router (DMI only).

Wizard Step 5: VSX Gateway Management

In the **VSX Gateway Management** window, define security policy rules that protect the VSX Gateway.

This policy is installed automatically on the new VSX Gateway.

Note - This policy applies **only** to traffic destined for the VSX Gateway. Traffic destined for Virtual Systems, other Virtual Devices, external networks, and internal networks is not affected by this policy.

The security policy consists of predefined rules for these services:

- **UDP** - SNMP requests
- **TCP** - SSH traffic
- **ICMP** - ICMP Echo (ping)
- **TCP** - HTTPS traffic

Completing the VSX Wizard

Click **Next** to continue and then click **Finish** to complete the VSX Gateway wizard.

This may take several minutes to complete.

A message shows successful or unsuccessful completion of the process.

If the process ends unsuccessfully, click **View Report** to see the error messages.

See *"VSX Diagnostics and Troubleshooting" on page 283*.

Configuring the Security Policy

1. **Allow**: Select to pass traffic on the selected services.

   Clear this option to block traffic on this service.

   By default, all services are blocked.

   For example, to be able to ping the VSX Gateway from the Management Server, allow ICMP traffic.

2. **Source**: Click the arrow and select a **Source Object** from the list.

   The default value is ***Any**.

   Click **New Source Object** to define a new source.

Working with VSX Gateways

In This Section:

Changing VSX Gateway Definitions 104
Deleting a VSX Gateway 108
Backing up and Restoring VSX Gateway 108

A VSX Gateway is a physical machine that serves as a container for Virtual Systems and other virtual network components.

This section has step-by-step procedures for creating and configuring standalone VSX Gateways.

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.
- Virtual Routers are not supported (Known Limitation 01413513).

Changing VSX Gateway Definitions

After you create a VSX Gateway, you can modify the topology, other parameters, and advanced configurations in the **VSX Gateway Properties** window.

To open this window, double-click on the VSX Gateway object in SmartConsole.

The **VSX Gateway Properties** window opens.

VSX Gateway - General Properties

In the **General Properties** page, check and re-establish the SIC trust, and activate Check Point products for this VSX Gateway.

You can change these properties:

- **Comment** - Free text description for the Object List and elsewhere.
- **Color** - Color of the object icon as it appears in the Object Tree.
- **Secure Internal Communication** - Check and re-establish the SIC trust.
- **Check PointProducts** - Select Check Point products for this VSX Gateway.

Secure Internal Communication (SIC)

You can test and reset the SIC trust and also see the VSX Gateway Relative Distinguished Name.

To initialize the SIC trust:

1. In **Gateways & Servers** view or **Object Explorer**, double-click the VSX Gateway.

   You can also search for the VSX Gateway in the **Object Explorer**.
2. In the **VSX Gateway Properties** window, click **Communication**.
3. In the **Trusted Communication** window, enter and confirm the SIC Activation Key.
4. Click **Initialize**.

Note - If you cannot establish trust, click **Test SIC Status** to see the reason for the failure. The most common issues are an incorrect activation key and connectivity problems between the Management Server and the VSX Gateway.

To reset the SIC trust with the VSX Gateway:

1. From the VSX Gateway CLI, use the `cpconfig` utility to re-initialize the SIC.
2. In the **Communication** window, click **Reset**.
3. Click **Yes** in the confirmation window.
4. Enter and confirm the SIC authentication password.
5. Click **Initialize**.
6. Install the applicable policy (*<Name of VSX Gateway Object>_VSX*) on the VSX Gateway object only.
7. On the VSX Gateway CLI, run: `cpstop;cpstart`

Check Point Software Blades

Select the Check Point Software Blades to install on this VSX Gateway from the list. The items you see are available for the product version and your license agreement.

VSX Gateway - Physical Interfaces

The **Physical Interfaces** page lets you add or delete a physical interface on the VSX Gateway, and to define a VLAN trunk.

- To add a new physical interface, click **Add** and enter the interface name in the appropriate field.

- To remove a physical interface, select the interface and click **Remove**.
- To define an interface as a VLAN trunk, select **VLAN Trunk** for the interface.

VSX Gateway - Topology

The **Topology** page contains definitions for interfaces and routes between interfaces and Virtual Devices.

Interfaces

The Interfaces section defines interfaces and links to devices. You can add new interfaces, and delete or modify existing interfaces.

To add an interface:

1. Click **New** and select one of these options:
   - **Regular** - Create a new interface
   - **Leads to Virtual Router**
   - **Leads to Virtual Switch**

   The **Interface Properties** window opens.

   Click **Actions** > **Copy to Clipboard** to copy the **Interfaces** table in CSV format.
2. Define the appropriate properties. See *"Working with Interface Definitions" on page 147*.
3. Click **OK**.

Routes

The **Routes** section of the **Topology** window defines routes between network devices, network addresses, and Virtual Devices. Some routes are defined automatically based on the interface definitions. You can add, change, and delete routes.

To add a default route to the routing table:

1. Click **Add Default Route**.

   The **Default Gateway** window opens.
2. Enter the default route IP address or select the default Virtual Router.
3. Click **OK**.

   The default route is added to the routing table.
4. Select the default route and click **Edit**.

   The **Route Configuration** window opens.

5. Configure the settings for the default route.
6. Click **OK**.

To add a new route to the routing table:

1. Click **Add**.

   The **Route Configuration** window opens.
2. Configure the **Destination** IP address and netmask.
3. Configure the next hop IP address or Virtual Router.
4. **Optional:** Select **Propagate route to adjacent Virtual Devices** to "advertise" the route to neighboring Virtual Devices, and enable connectivity between them.
5. Click **OK**.

To change a route:

1. Select the route.
2. Click **Edit**.

   The **Route Configuration** window opens.
3. Change the settings.
4. Click **OK**.

To delete a route:

1. Select the route.
2. Click **Remove**.

   A confirmation window opens.
3. Click **OK**.

Topology Calculation

Select the **Calculating topology automatically based on routing information** option to let VSX automatically calculate the network topology based on interface and routing definitions. When enabled, VSX creates automatic links, or connectivity cloud objects linked to existing internal or external networks.

- This option is not available in Bridge Mode.
- We recommend that you do not use this option with dynamic routing configurations.

Note - If you wish to enable Anti-Spoofing protection when there are no routes pointing to internal networks, disable the **Calculating topology automatically based on routing information** option. Modify the appropriate interface definitions to enable Anti-Spoofing.

Deleting a VSX Gateway

When you delete a VSX Gateway object, the operation automatically deletes all Virtual Systems and other Virtual Devices associated with that VSX Gateway from the management database.

To delete a VSX Gateway:

1. From the **Gateways & Servers**view or Object Explorer tree, right-click the VSX Gateway object on the Object Tree and select **Delete**.
2. In the window that opens, click **Yes**.

Backing up and Restoring VSX Gateway

In the event of a catastrophic VSX Gateway failure, you can restore the VSX Gateway configuration and its Virtual Device configuration.

Follow the instructions in the sk100395: How to backup and restore VSX Gateway.

Working with Virtual Systems

In This Section:

Introduction 109
Creating a New Virtual System 110
Modifying a Virtual System 113
Configuring Bridge Interfaces in Regular Virtual Systems 116
Deleting a Virtual System 118
Configuring DNS Servers on a Virtual System 119
Configuring DHCP Server on a Virtual System 127

This section presents procedures for creating and configuring Virtual Systems.

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.
- Virtual Routers are not supported (Known Limitation 01413513).

Introduction

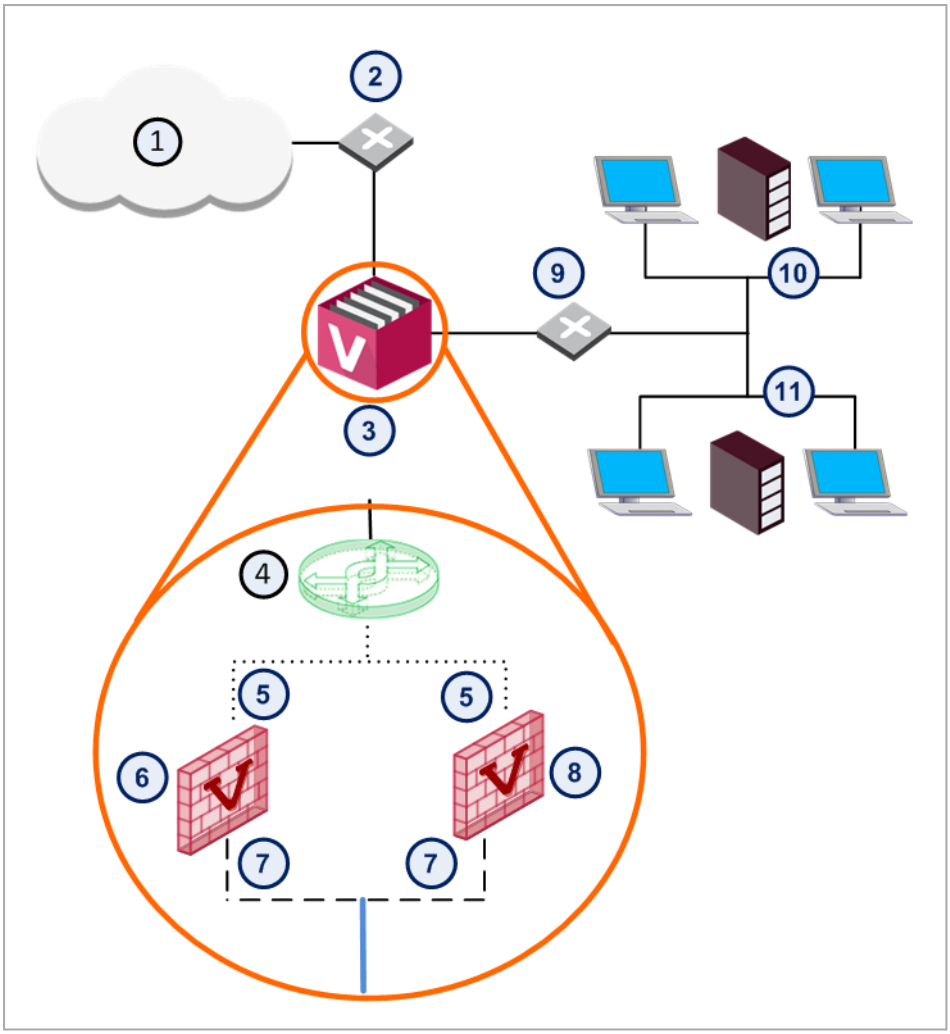
The Virtual System definition process varies somewhat according to the template selected when creating the VSX Gateway.

A typical Virtual System contains two interfaces:

- **External interface** leading to external networks, a DMZ, or the Internet
- **Internal interface** leading to internal networks or servers, often by means of a VLAN trunk

Important - For the maximum supported number of interfaces, see the *R82 Release Notes* > Chapter "Maximum Supported Items".

Here is an example of a typical VSX Gateway deployment with two Virtual Systems, each with two interfaces.



Item	Description		Item	Description
1	Internet		8	Virtual System 2
2	Router		9	VLAN Switch
3	VSX Gateway		10	Network 1
4	Virtual Switch		11	Network 2
5	External Interface		-----	VLAN Interface
6	Virtual System 1		———	VLAN Trunk
7	Internal Interface		.....	Warp Link

Creating a New Virtual System

You use the **Virtual Systems Wizard** to create a new Virtual System. Modify the initial definition and configure advanced options after you complete the wizard.

To start the Virtual System wizard:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the new Virtual System.
2. From the left navigation panel, click **Gateways & Servers**.
3. Create a new Virtual System object in one of these ways:
   - From the top toolbar, click the **New (✦) > VSX > New Virtual System**.
   - In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > VSX > New Virtual System**.
   - In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Virtual System**.

   The **Virtual System Wizard** opens.
4. Configure the applicable settings in the wizard as described below.
5. Install the applicable Access Control Policy on the new Virtual System object.

Wizard - Defining General Properties

The **General Properties** wizard page defines the Virtual System object and the hosting VSX Gateway.

These are the parameters in this page:

- **Name**: Unique, alphanumeric for the Virtual System. The name cannot contain spaces or special characters except the underscore.

  Note - The name of the VSX Gateway or VSX Cluster object must not exceed 26 characters.
- **VSX Gateway / Cluster**: Select the VSX Gateway that is hosting the Virtual System.
- **Bridge Mode**: Select this option to create a Virtual System in the Bridge Mode.

Wizard - Defining Network Configuration

In the **Virtual System Network Configuration** page, define internal and external interfaces and the IP address topology behind the internal interface.

Non-Bridge Mode

Important - From R81.10, it is possible:

- To add bridge interfaces to regular Virtual Systems in SmartConsole.
- To configure regular Virtual Systems without an IP address that contain only bridge interfaces.

See *"Configuring Bridge Interfaces in Regular Virtual Systems" on page 116*.

To configure the external and internal interfaces:

1. In the **Interfaces** section, configure the applicable interfaces.

   You can add interfaces, delete, and change interfaces.

   To add an interface, click **Add**, select an interface type from the list and configure its properties.

2. Select the **Main IP Address** from the list.

   This IP address is usually assigned to the external interface and specifies the Virtual System address used with NAT or VPN connections.

   To make an external IP address routable, select the external interface IP address as the main IP address.

3. Define network routing for your deployment.

   Some routes are automatically defined by the interface definitions.

   For example, you define a default gateway route leading to an external Virtual Router or to the Virtual System external interface.

   To manually add a default route to the **Routes** table, click **Add Default Routes**.

   Enter the default route IP address, or select the default Virtual Router.

   The **Route Configuration** window opens.

4. Complete the definition.

Bridge Mode

Interfaces: To configure the external and internal interfaces, define interfaces and links to devices in the **Interfaces** section. You can add, change, and remove interfaces. To add an interface, click **Add**. The **Interface Properties** window opens. Select an interface from the list and define is properties.

Wizard - Completing the Definition

Click **Next** and then click **Finish** to create the Virtual System.

Note that this may take several minutes to complete.

A message appears indicating successful or unsuccessful completion of the process.

If the process ends unsuccessfully, click **View Report** to view the error messages.

For further assistance, see *"VSX Diagnostics and Troubleshooting" on page 283*.

After you create a Virtual System using the Virtual System Wizard, you can modify the topology and all other parameters (except the name of the Virtual System) using the **Virtual System Properties** window.

Modifying a Virtual System

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server used to manage the Virtual System.
2. From the **Gateways & Servers** view or **Object Explorer**, double-click the Virtual System object.
3. Configure the applicable settings as described below.
4. Click **OK** to push the VSX Configuration.
5. Install the applicable Access Control Policy on the new Virtual System object.

General Properties

The **General Properties** page lets you specify the main IP address and to enable various Check Point products for a Virtual System.

Topology

The **Topology** page contains definitions for Virtual System interfaces, routes and Warp Links. Based on these interface settings, VSX automatically creates routes to Virtual Devices and the VSX Gateway.

Note - If you modify the topology for a specific Virtual System in a cluster environment, the cluster topology is not updated until you install a policy on that Virtual System.

- **Interfaces**: The **Interfaces** section defines interfaces and links to devices. You can add new interfaces as well as delete and modify existing interfaces.

  To add an interface, click **New** and select one of these options:

  - **Regular** - To select a physical interface
  - **Leads to Virtual Router** - To attach this Virtual System to a Virtual Router
  - **Leads to Virtual Switch** - To attach this Virtual System to a Virtual Switch
  - **Bridge** - From R81.10, it is possible to add bridge interfaces to regular Virtual Systems in SmartConsole. See *"Configuring Bridge Interfaces in Regular Virtual Systems" on page 116*.

The **Interface Properties** window opens. Select the interface from the list and define the appropriate properties. The section *"Working with Interface Definitions" on page 147* and the SmartConsole online help provide explanations of the various properties and options.

Click **Actions** > **Copy to Clipboard** to copy the **Interfaces** table in CSV format.

- **Routes**: To add a default route to the Routes table, click **Add Default Routes** and either enter an IP address or select a Virtual Router. The **Route Configuration** window opens. Click **Help** for details regarding the various properties and options. You can also add, change and remove routes (see *"Working with VSX Gateways" on page 104*).
- **Calculate topology automatically based on routing information**: Enable this option to allow VSX to automatically calculate the network topology based on interface and routing definitions (enabled by default). VSX creates automatic links, or connectivity cloud objects linked to existing internal or external networks.
  - When this option is enabled, you cannot configure the topology using **Topology** tab in the **Interface Properties** window. These options are not available on the tab.
  - This option is not available in the Bridge Mode.
  - When employing dynamic routing, it is recommended to disable this option.
- **VPN Domain**: The VPN Domain defines the set of hosts located behind a given Virtual System that communicate via a VPN tunnel with peer Virtual Systems. These options are only available if you selected **VPN** in the **Check Point Products** section on the **General Properties** page.

  When including a Virtual Device as part of a VPN connection, you must specify a VPN Domain. The domain definition specifies Virtual System interfaces that are included in the VPN.

  You can define a VPN Domain by enabling the applicable option:
  - **All IP Addresses behind gateway based on topology information**: Includes all hosts not located behind an external VSX Gateway interface.
  - **Manually Defined**: Includes all hosts in the selected network or group.

NAT > Advanced

On the **NAT** > **Advanced** page, you configure NAT rules for packets originating from a Virtual System.

To enable and configure NAT for a Virtual System:

1. Select **Add Automatic Address Translation**.
2. Select a translation method:
   - **Hide**: Hide NAT only allows connections originating from the internal network. Internal hosts can access internal destinations, the Internet and other external networks. External sources cannot initiate a connection to internal network addresses.
   - **Static**: Static NAT translates each private address to a corresponding public address.
3. If you select **Hide**, select one of these options:
   - **Hide behind Gateway** hides the real IP address behind the Virtual System external interface IP address,

     or
   - **Hide behind IP Address** hides the real address behind a virtual IP address, which is a routable, public IP address that does not belongs to any real machine.
4. If you selected **Static NAT**, enter the static IP address in the appropriate field.
5. Select the VSX Gateway from the **Install on Gateway** list.

In addition, see *"Working with Network Address Translation (NAT)" on page 169*.

Configuring Bridge Interfaces in Regular Virtual Systems

To add a new bridge interface

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual System.
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the Virtual System object.
4. From the left tree, click **Topology**.
5. In the **Interfaces** section, click **New** and select **Bridge**.
6. On the **General** tab, in the **Interface** field, select the first subordinate interface (for example, `eth2`).

   On other tabs, configure the applicable settings and click **OK**.
7. In the **Interfaces** section, click **New** and select **Bridge**.
8. On the **General** tab, in the **Interface** field, select the second subordinate interface (for example, `eth3`).

   On other tabs, configure the applicable settings and click **OK**.
9. Click **OK** to push the VSX Configuration.
10. Install the applicable Access Control Policy on the Virtual System object.

Important:

- A bridge interface contains only two subordinate interfaces.
- In each bridge interface you must configure these **Topology** settings:
  - One subordinate interface must have the configuration **External (leads out to the Internet)**
  - One subordinate interface must have the configuration **Internal (leads to the local network)** and **Not Defined**
- When a Virtual System contains only two interfaces configured as bridge subordinate interfaces, the Virtual System attaches them automatically to create a Layer 2 bridge interface.
  This configuration supports bridge subordinate interfaces (one or two) that are VLAN interfaces.
- To configure more than one bridge interface in a Virtual System, these conditions apply:
  1. All bridge subordinate interfaces must be VLAN interfaces with VLAN tags that the Virtual System can pair.
     The Virtual System attaches the bridge subordinate interfaces automatically based on their VLAN tags to create a bridge interface.
     Examples:
     - eth1.*111* and eth2.*111*
     - eth1.*222* and eth2.*222*
  2. The VLAN subordinate interfaces in all bridge interfaces in the Virtual System must belong to the same two physical VLAN trunks.
     Each bridge must contain VLAN interfaces with the same VLAN tag, but a different VLAN Trunk.
- You cannot configure a regular Virtual System with bridge in a VSX Cluster in the Active/Active Bridge Mode.

To edit bridge subordinate interfaces

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual System.
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the Virtual System object.
4. From the left tree, click **Topology**.
5. In the **Interfaces** section, select the bridge subordinate interface and click **Edit**.
6. Configure the applicable bridge interface settings.
7. Click **OK** to close the **Interface Properties** window.
8. Click **OK** to push the VSX Configuration.
9. Install the applicable Access Control Policy on the Virtual System object.

To delete a bridge interface

1. Determine the applicable bridge subordinate interfaces:
   a. Connect to the command line on the VSX Gateway (each VSX Cluster Member).

      On Scalable Platforms, you must connect to the Gaia Portal of the applicable Security Group.

   b. Log in to Gaia Clish.

      On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

   c. Go to the context of the Virtual System:

      ```
      set virtual-system<VSID>
      ```

   d. Examine the bridge interfaces:

      ```
      show bridging groups
      ```

2. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual System.
3. From the left navigation panel, click **Gateways & Servers**.
4. Open the Virtual System object.
5. From the left tree, click **Topology**.
6. In the **Interfaces** section:
   a. Select the first bridge subordinate interface > click **Delete** > click **OK** to confirm.
   b. Select the second bridge subordinate interface > click **Delete** > click **OK** to confirm.
7. Click **OK** to push the VSX Configuration.
8. Install the applicable Access Control Policy on the Virtual System object.

Deleting a Virtual System

To delete a Virtual System:

1. From the **Gateways & Servers**view or Object Explorer tree, right-click the Virtual System object and select **Delete**.
2. In the window that opens, click **Yes**.

Configuring DNS Servers on a Virtual System

Gaia uses the Domain Name Service (DNS) to translate host names into IP addresses.

To enable DNS lookups, you must enter the primary DNS server for your system. You can also enter secondary and tertiary DNS servers.

When the system resolves host names, it consults the primary name server. If a failure or time-out occurs, the system consults the secondary name server, and if necessary, the tertiary.

You can also define a DNS Suffix, which is a search for host-name lookup.

From R81, you can configure each Virtual System:

- **To use specific DNS Servers for all DNS queries**

  A Virtual System uses the specific configured DNS servers for all DNS queries.

- **To use specific DNS Servers for DNS queries sent for specific Domains**

  A Virtual System uses the configured DNS Forwarding Domain.

  The DNS Forwarding Domain determines the Domain Suffix and the DNS Servers for this Domain Suffix:

  - For all DNS queries that end with the Forwarding Domain Suffix, a Virtual System uses the specific DNS servers configured for this Forwarding Domain Suffix.
  - For all other DNS queries, a Virtual System uses other specific DNS servers configured in the Virtual System.

  Note - If a Domain in a DNS query contains a shorter Domain as its suffix, then for all DNS queries that end with the longer Domain's suffix a Virtual System uses the DNS servers configured to the longest Domain's match. For example, if you configured the Domain Suffixes "`com`" and "`checkpoint.com`" and their corresponding DNS servers, then for a DNS query with the suffix "`support.checkpoint.com`", a Virtual System uses the DNS server configured for the Domain Suffix "`checkpoint.com`" and not the DNS server configured for the Domain Suffix "`com`".

- **To work as a DNS Relay**

  A Virtual System listens to DNS queries on specific interfaces and forwards them through all other interfaces (all these interfaces belong to the same Virtual System).

Important:

- You can configure one or all of the above specific DNS settings on a Virtual System.
  To configure and use any of the above specific DNS settings, you must enable the entire feature on the VSX Gateway (each VSX Cluster Member).
- By default, this feature is disabled:
  All Virtual Systems you create use the global DNS settings configured on the VSX Gateway or VSX Cluster Member.
- When you enable this feature:
  a. The default DNS settings in the context of VS0 become the same as the global DNS settings configured on the VSX Gateway or VSX Cluster Member.
  b. The default DNS settings in the context of every new Virtual System become the same as the DNS settings in the context of VS0.
- When you disable this feature:
  The global DNS settings on the VSX Gateway or VSX Cluster Member become the same as the DNS settings in the context of VS0.
- You must configure all DNS settings in Gaia Clish on the VSX Gateway (each VSX Cluster Member).
- In a VSX Cluster, you must configure all the VSX Cluster Members in the same way.
- Some programs that use POSIX sockets to resolve hostnames (for example, `ping` and `ssh`) fail to do so when they resolve names without "`.`" in them. These programs rely on the DNS search suffix.
- For Software Blades that require contracts or updates to function, you must configure the DNS servers in the context of the VSX Gateway or VSX Cluster Member itself (context of VS0). For additional information, see sk106496.

Enabling or disabling the feature

1. Connect to the command line on the VSX Gateway (each VSX Cluster Member).

   On Scalable Platforms, you must connect to the Gaia Portal of the applicable Security Group.

2. Log in to Gaia Clish.

   On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

3. Enable ("`per-vs`") or disable ("`default`") the feature:

   Note - You can run this command in the context of any Virtual Device.

   ```
   set dns mode {per-vs | default}
   ```

4. Show the status of the feature:

```
show dns mode
```

5. Save the changes:

```
save config
```

Configuring specific DNS settings for all DNS queries

1. Connect to the command line on the VSX Gateway (each VSX Cluster Member).

   On Scalable Platforms, you must connect to the Gaia Portal of the applicable Security Group.

2. Log in to Gaia Clish.

   On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

3. Enable the feature:

```
set dns mode per-vs
show dns mode
```

4. Go to the context of the applicable Virtual System:

```
set virtual-system <VSID>
```

5. Configure the DNS Servers and the DNS Suffix:

```
set dns
      primary <IPv4 or IPv6 Address>
      secondary <IPv4 or IPv6 Address>
      tertiary <IPv4 or IPv6 Address>
      suffix <Name for Local Domain>
```

6. Show the configured settings:

```
show dns
```

7. Save the changes:

```
save config
```

To delete the configured settings

```
set virtual-system <VSID>
delete dns
      primary
      secondary
      tertiary
      suffix
save config
```

Example

```
set dns mode per-vs
set virtual-system 1
set dns primary 192.168.10.21
set dns secondary 192.168.10.22
set dns tertiary 192.168.10.23
set dns suffix mycompany.com
show dns
save config
```

Configuring specific DNS settings for specific Domains

1. Connect to the command line on the VSX Gateway (each VSX Cluster Member).

   On Scalable Platforms, you must connect to the Gaia Portal of the applicable Security Group.

2. Log in to Gaia Clish.

   On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

3. Enable the feature:

   ```
   set dns mode per-vs
   show dns mode
   ```

4. Go to the context of the applicable Virtual System:

   ```
   set virtual-system <VSID>
   ```

5. Configure the DNS Servers and the DNS Suffix for all DNS queries:

   ```
   set dns
         primary <IPv4 or IPv6 Address>
         secondary <IPv4 or IPv6 Address>
         tertiary <IPv4 or IPv6 Address>
         suffix <Name for Local Domain>
   ```

6. Show the configured settings for all DNS queries:

```
show dns
```

7. Configure the Forwarding Domain Suffix:

```
add dns proxy forwarding-domain <Domain Suffix>
```

8. Configure the DNS Servers for the specific Forwarding Domain Suffix:

```
set dns proxy forwarding-domain <Domain Suffix>
      primary <IPv4 or IPv6 Address>
      secondary <IPv4 or IPv6 Address>
      tertiary <IPv4 or IPv6 Address>
```

9. Show the configured Forwarding Domain Suffixes:

```
show dns proxy forwarding-domains
```

10. Show the configured settings for the specific Forwarding Domain Suffix:

```
show dns proxy forwarding-domain <Domain Suffix>
      primary
      secondary
      tertiary
```

11. Save the changes:

```
save config
```

To delete the configured settings

```
set virtual-system <VSID>
delete dns
      primary
      secondary
      tertiary
      suffix
save config
```

```
set virtual-system <VSID>
delete dns proxy forwarding-domain <Domain Suffix>
save config
```

```
set virtual-system <VSID>
delete dns proxy forwarding-domain <Domain Suffix>
      primary
      secondary
      tertiary
save config
```

Example

```
set dns mode per-vs
set virtual-system 1
set dns primary 192.168.10.21
set dns secondary 192.168.10.22
set dns tertiary 192.168.10.23
set dns suffix mycompany.com
show dns
add dns proxy forwarding-domain anothercompany.com
set dns proxy forwarding-domain anothercompany.com primary 172.16.30.41
set dns proxy forwarding-domain anothercompany.com secondary 172.16.30.42
set dns proxy forwarding-domain anothercompany.com tertiary 172.16.30.43
show dns proxy forwarding-domains
show dns proxy forwarding-domain anothercompany.com primary
show dns proxy forwarding-domain anothercompany.com secondary
show dns proxy forwarding-domain anothercompany.com tertiary
save config
```

Configuring a Virtual System to work as a DNS Relay

1. Connect to the command line on the VSX Gateway (each VSX Cluster Member).

   On Scalable Platforms, you must connect to the Gaia Portal of the applicable Security Group.

2. Log in to Gaia Clish.

   On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

3. Enable the feature:

   ```
   set dns mode per-vs
   show dns mode
   ```

4. Go to the context of the applicable Virtual System:

   ```
   set virtual-system <VSID>
   ```

5. Configure the DNS Servers and the DNS Suffix for all DNS queries:

   ```
   set dns
         primary <IPv4 or IPv6 Address>
         secondary <IPv4 or IPv6 Address>
         tertiary <IPv4 or IPv6 Address>
         suffix <Name for Local Domain>
   ```

6. Show the configured settings:

```
show dns
      primary
      secondary
      tertiary
      suffix
```

7. Configure the interfaces, on which the Virtual System must listen to DNS queries:

```
add dns proxy listening-interface <Name of Virtual System Interface>
```

8. Show the configured listening interfaces:

```
show dns proxy listening-interfaces
```

9. Save the changes:

```
save config
```

To delete the configured settings

```
set virtual-system <VSID>
delete dns
      primary
      secondary
      tertiary
      suffix
save config
```

```
set virtual-system <VSID>
delete dns proxy listening-interface <Name of Virtual System Interface>
save config
```

Example

```
set dns mode per-vs
set virtual-system 1
set dns primary 192.168.10.21
set dns secondary 192.168.10.22
set dns tertiary 192.168.10.23
set dns suffix mycompany.com
show dns
add dns proxy listening-interface wrp128
show dns proxy listening-interfaces
save config
```

CLI Parameters

Parameter	Description
`mode {per-vs | default}`	Enables ("`per-vs`") or disables ("`default`") the feature.
`primary <IPv4 or IPv6 Address>`	Specifies the IPv4 or IPv6 address of the primary DNS server, which resolve host names. This must be a host that runs a DNS server.
`secondary <IPv4 or IPv6 Address>`	Specifies the IPv4 or IPv6 address of the secondary DNS server, which resolves host names if the primary server does not respond. This must be a host that runs a DNS server.
`tertiary <IPv4 or IPv6 Address>`	Specifies the IPv4 or IPv6 address of the tertiary DNS server, which resolves host names if the primary and secondary servers do not respond. This must be a host that runs a DNS server.
`suffix <Name for Local Domain>`	Specifies the name that is put at the end of all DNS searches if they fail. By default, it must be the local domain name. A valid domain name suffix is made up of subdomain strings separated by periods. Subdomain strings must begin with an alphabetic letter and can consist only of alphanumeric characters and hyphens. The domain name syntax is described in RFC 1035 (modified slightly in RFC 1223). **Note** - Domain names that are also valid numeric IP addresses (for example: 10.19.76.100), although syntactically correct, are not permitted. Example: You configured the DNS Suffix "`example.com`" and you try to ping the host "`foo`" (with the command "`ping foo`"). If Gaia cannot resolve "`foo`", then Gaia tries to resolve "`foo.example.com`".

Parameter	Description
`forwarding-domain <Domain Suffix>`	Specifies the Forwarding Domain Suffix. The DNS Forwarding Domain determines the Domain Suffix and the DNS Servers for this Domain Suffix: ■ For all DNS queries that end with the Forwarding Domain Suffix, a Virtual System uses the specific DNS servers configured for this Forwarding Domain Suffix. ■ For all other DNS queries, a Virtual System uses other specific DNS servers configured in the Virtual System.
`listening-interface <Name of Virtual System Interface>`	Specifies the name of a Virtual System interface, on which the Virtual System must listen to DNS queries.

Configuring DHCP Server on a Virtual System

1. Connect to the command line on the VSX Gateway / each VSX Cluster Member.

   On Scalable Platforms, you must connect to the Gaia Portal of the applicable Security Group.

2. Log in to Gaia Clish.

   On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

3. Go to the context of the applicable Virtual System:

   ```
   set virtual-system <VS ID>
   ```

4. Configure the required DHCP Server settings as described in the *R82 Gaia Administration Guide* > Chapter "Network Management" > Section "DHCP Server" > Section "Configuring a DHCP Server in Gaia Clish".

Working with Virtual Switches

In This Section:

Introduction 128
Creating a New Virtual Switch 129
Modifying a Virtual Switch 130
Deleting a Virtual Switch 131

This section describes how to define and configure a Virtual Switch.

Note - In Security Groups in Maestro and Scalable Chassis:

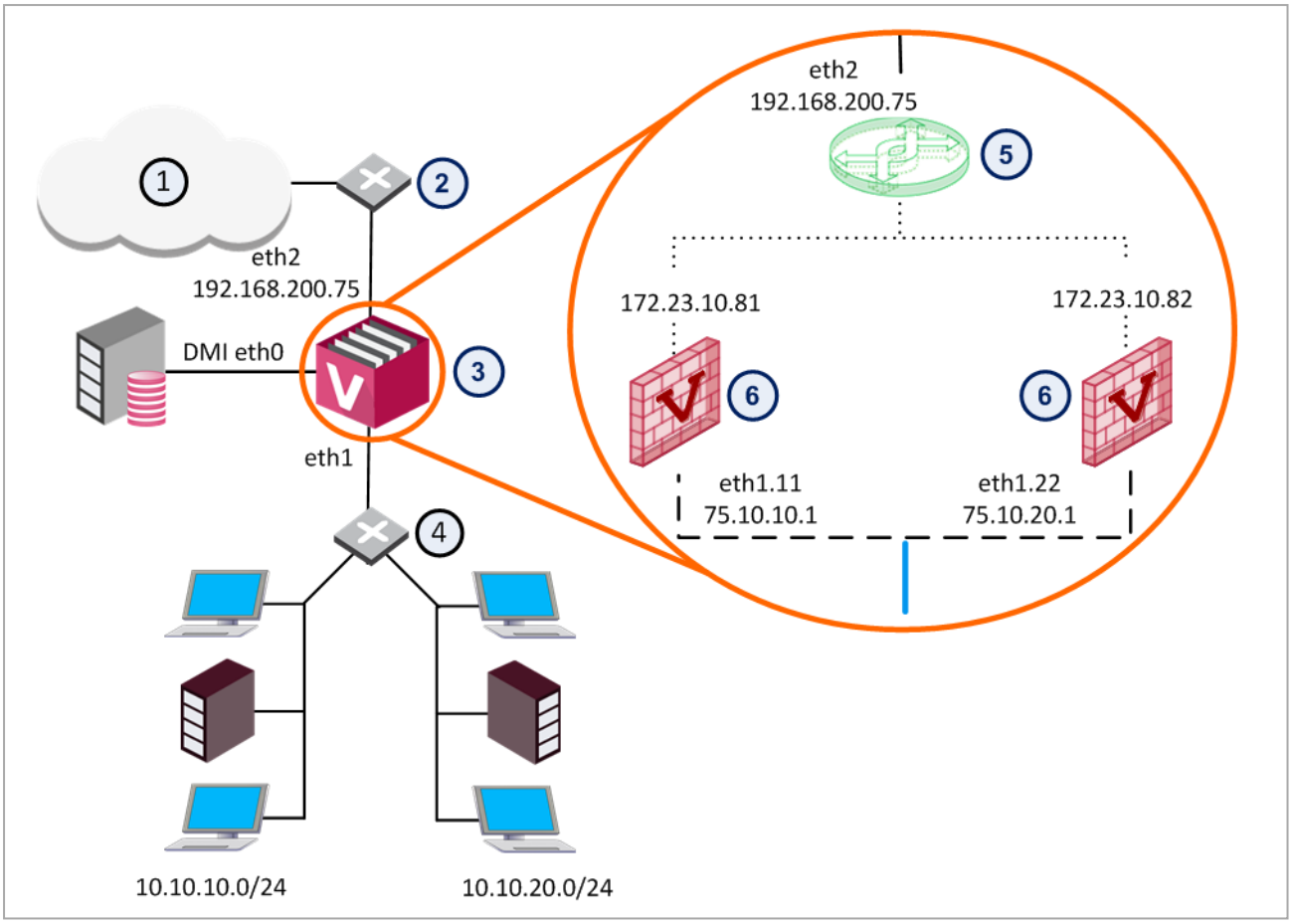
- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.

Introduction

Virtual Switches provide level-2 connectivity between Virtual Systems and internal or external networks.

As with physical switches, each Virtual Switch maintains a forwarding table containing entries that describe known networks and directions for reaching them.

You can define Virtual Switches for external and internal communications.



Item	Description		Item	Description
1	Internet		6	Virtual Systems
2	Router		-----	VLAN Interface
3	VSX Gateway		———	VLAN Trunk
4	VLAN Switch		.....	Warp Link
5	Virtual Switch			

The figure shows a typical deployment using a Virtual Switch for external connections and a VLAN trunk leading to the internal, protected network.

Creating a New Virtual Switch

Use the **Virtual Switch Wizard** to create a new Virtual Switch. You can modify the initial definition and configure advanced options after completing the wizard.

To create a new Virtual Switch:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the new Virtual System.
2. From the left navigation panel, click **Gateways & Servers**.
3. Create a new Virtual Switch object in one of these ways:
   - From the top toolbar, click the **New (✦) > VSX > New Virtual Switch**.
   - In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > VSX > New Virtual Switch**.
   - In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Virtual Switch**.

   The **Virtual Switch Wizard** opens.
4. In the **Name** field, enter the name for the new Virtual Switch.
5. In the **VSX Gateway / Cluster** field, select the applicable VSX Gateway or VSX Cluster.
6. Click **Next**.
7. In the **Interfaces** section, click **Add** to add the interface, to which the Virtual Switch connects.
8. Click **Next**.
9. Click **Finish**.

Modifying a Virtual Switch

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual Switch.
2. From the **Gateways & Servers** view or **Object Explorer**, double-click the Virtual Switch object.

Virtual Switch - General Properties

The **General Properties** page allows you to add comments and change the icon color as displayed in SmartConsole.

Virtual Switch - Topology

The **Topology** page defines Virtual Switch interfaces. You can only modify the single defined interface. You cannot change the settings for Warp interfaces in this window.

To add an interface:

1. Click **New**.

   The **Interface Properties** window opens.

2. Select an interface from the list and define the IP address, net mask and other properties.
3. **Optional:** Click **Actions** > **Copy to Clipboard** to copy the **Interfaces** table in CSV format.

Deleting a Virtual Switch

To delete a Virtual Switch:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the new Virtual Switch.
2. From the **Gateways & Servers** view or **Object Explorer**, double-click the Virtual Switch object.
3. From the left tree, click **Topology**.
4. In the **Interfaces** section, remove all interfaces.
5. Click **OK**.
6. Right-click the Virtual Switch object and select **Delete**.
7. Click **Yes** in the confirmation box.
8. Publish the SmartConsole session.

Working with Virtual Routers

In This Section:

Introduction 132

Creating a New Virtual Router 135

Modifying a Virtual Router Definition 135

Deleting a Virtual Router 136

Virtual Routers in Virtual System Load Sharing Mode 136

This section describes how to define and configure a Virtual Router.

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.
- Virtual Routers are not supported (Known Limitation 01413513).

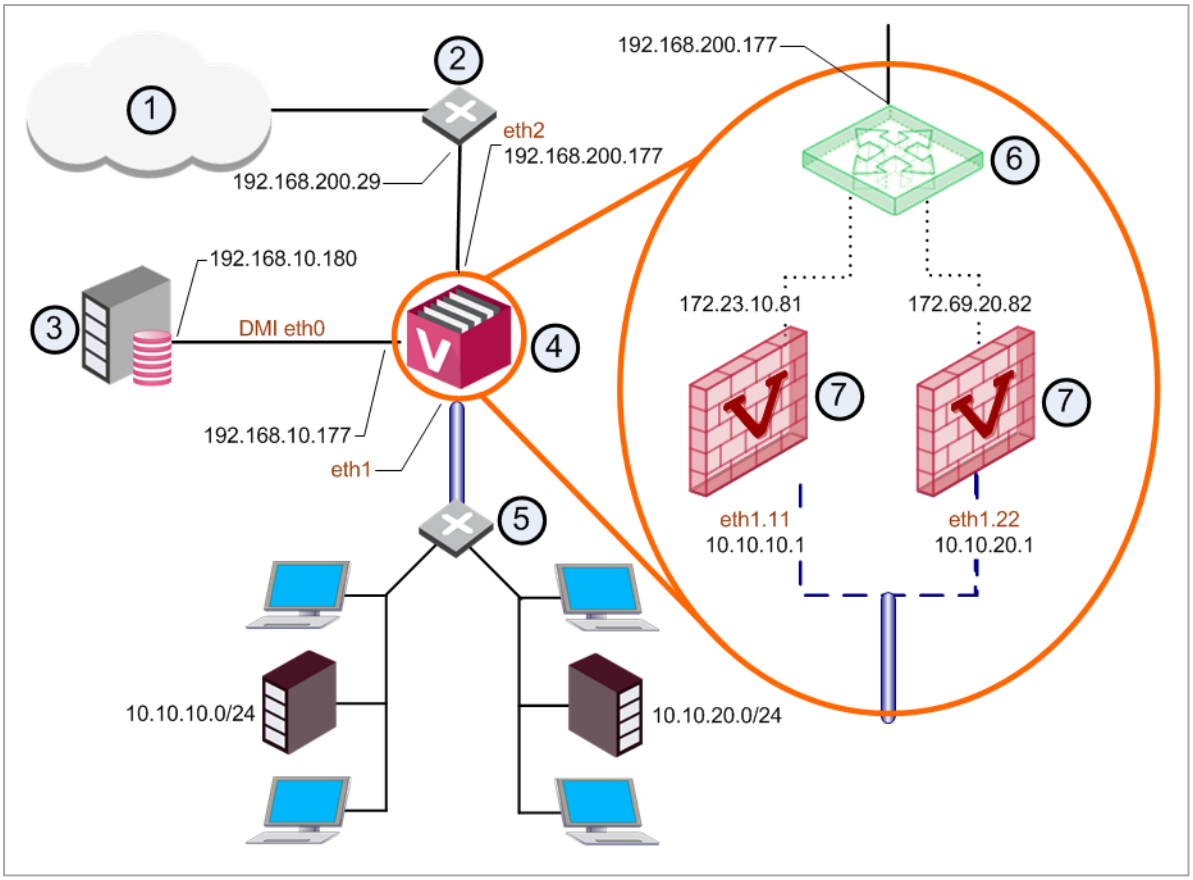
Introduction

As with physical routers, each Virtual Router maintains a routing table containing entries that describe known networks and directions on how to reach them.

You can define Virtual Routers for both external and internal communications.

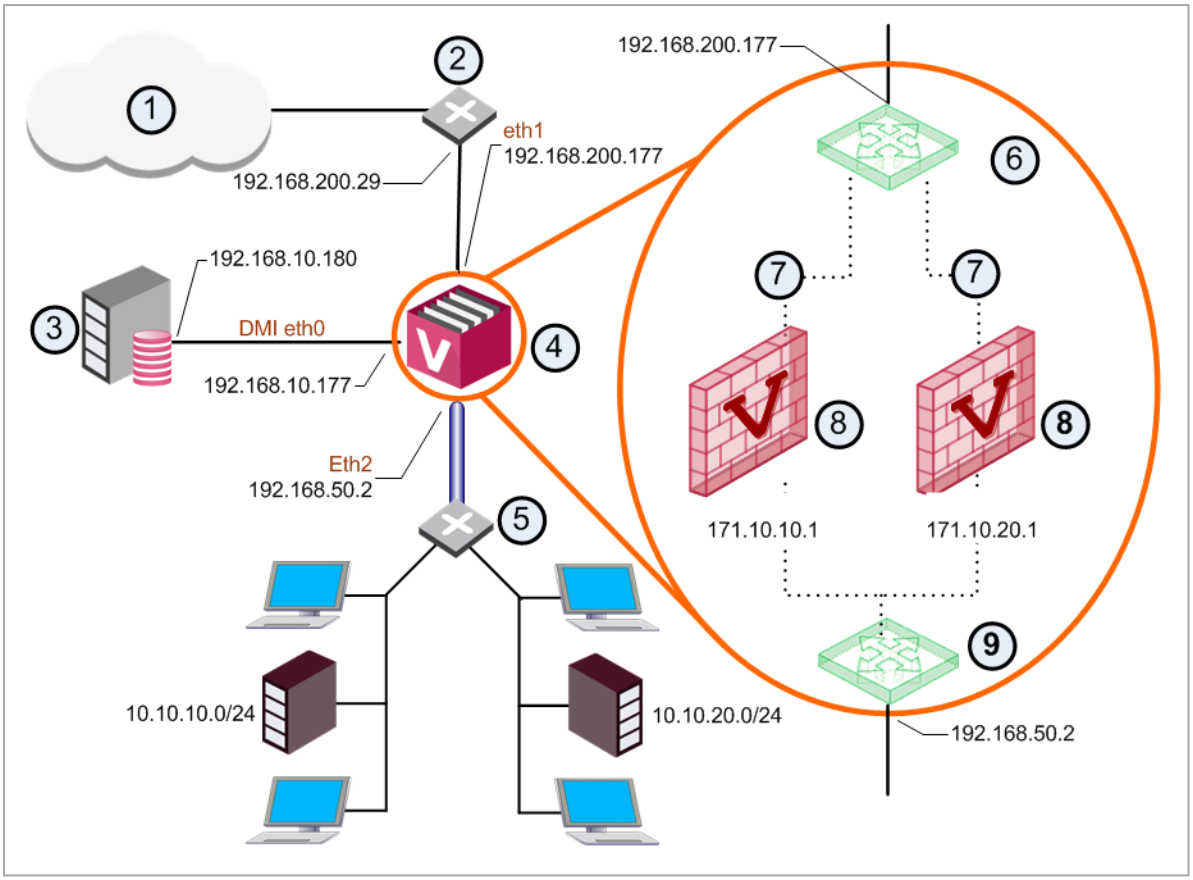
A Virtual Router that connects to external networks, including a DMZ and the Internet, are referred to as an external Virtual Router.

A Virtual Router that connects to internal, protected networks is known as an internal Virtual Router.



Item	Description		Item	Description
1	Internet		6	External Virtual Router
2	Router		7	Virtual Systems
3	Security Management Server		-----	VLAN Interface
4	VSX Gateway		———	VLAN Trunk
5	VLAN switch		.....	Warp Link

An external Virtual Router functions as the external gateway for Virtual Systems, allowing them to share a single secure physical interface leading to external networks and the Internet.



Item	Description		Item	Description
1	Internet		7	Unnumbered
2	Router		8	Virtual Systems
3	Security Management Server		9	Internal Virtual Router
4	VSX Gateway		-----	VLAN Interface
5	Switch		———	VLAN Truck
6	External Virtual Router		.....	Warp link

In this scenario, VSX creates Warp interfaces between the Virtual Systems and both Virtual Routers. Note that the external Virtual System interfaces are defined as unnumbered interfaces.

An internal Virtual Router typically connects with one interface leading to internal networks through a switch with additional Warp Links leading to other Virtual Systems located in the VSX Gateway.

After you create a new Virtual Router, add new interfaces to the Virtual Systems to connect to the Virtual Router.

Creating a New Virtual Router

Use the Virtual Router Wizard to create a new Virtual Router. You can modify the initial definition and configure advanced options after you complete the wizard.

On interfaces and routes, you can select the **Propagate route to adjacent Virtual Devices** option to broadcast the IP address to neighboring Virtual Devices. This option enables connectivity with these Virtual Devices.

To create a Virtual Router:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the new Virtual System.
2. From the left navigation panel, click **Gateways & Servers**.
3. Create a new Virtual Router object in one of these ways:
   - From the top toolbar, click the **New (✳) > VSX > New Virtual Router**.
   - In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > VSX > New Virtual Router**.
   - In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Virtual Router**.

   The **Virtual RouterWizard** opens.
4. In the **Name** field, enter the name for the new Virtual Router.
5. In the **VSX Gateway / Cluster** field, select the applicable VSX Gateway or VSX Cluster.
6. Click **Next**.
7. In the **Interfaces** section, click **Add** to add the interface, to which the Virtual Router connects.
8. In the **Routes** section, click **Add** to add the applicable network routes.
9. **Optional:** Click **Add Default Route** and configure the default route.
10. Click **Next**.
11. Click **Finish**.

Modifying a Virtual Router Definition

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual Router.
2. From the **Gateways & Servers** view or **Object Explorer**, double-click the Virtual Router object.

Virtual Router - General Properties

The **General Properties** page enables you change the Virtual Router IP address as well as to add comments and change the icon color as displayed in SmartConsole.

Virtual Router - Topology

The **Virtual Router Network Configuration** page defines the network topology for the Virtual Router. For an external interface, you define one or more shared external interfaces and a default gateway.

Topology is defined by these properties:

- **Interfaces**: Add new interfaces, or modify or delete existing interfaces.

  To add an interface, click **New**. The **Interface Properties** window opens. Select an interface from the list and define the IP address, net mask and other properties (see *"Working with Interface Definitions" on page 147*).

- **Routes**: Add network routes between this Virtual Router, Virtual Systems, external network devices and network addresses. Some Warp Link routes are defined automatically and cannot be modified or deleted. You can manually add new routes as well as delete and modify non-Warp Link routes.

- **Add Default Route**: Define the default route as an IP address or Virtual System.

- **Advanced Routing**: Configure source-based routing rules. See *"Working with Source-Based Routing" on page 138*.

Deleting a Virtual Router

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the new Virtual Router.
2. From the **Gateways & Servers** view or **Object Explorer**, double-click the Virtual Router object.
3. From the left tree, click **Topology**.
4. In the **Interfaces** section, remove all interfaces.
5. Click **OK**.
6. Right-click the Virtual Router object and select **Delete**.
7. Click **Yes** in the confirmation box.
8. Publish the SmartConsole session.

Virtual Routers in Virtual System Load Sharing Mode

From R81, you can configure Virtual Routers in VSLS mode.

See *"Configuring Virtual System Load Sharing (VSLS)" on page 213*.

Working with Source-Based Routing

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.
- Virtual Routers are not supported (Known Limitation 01413513).

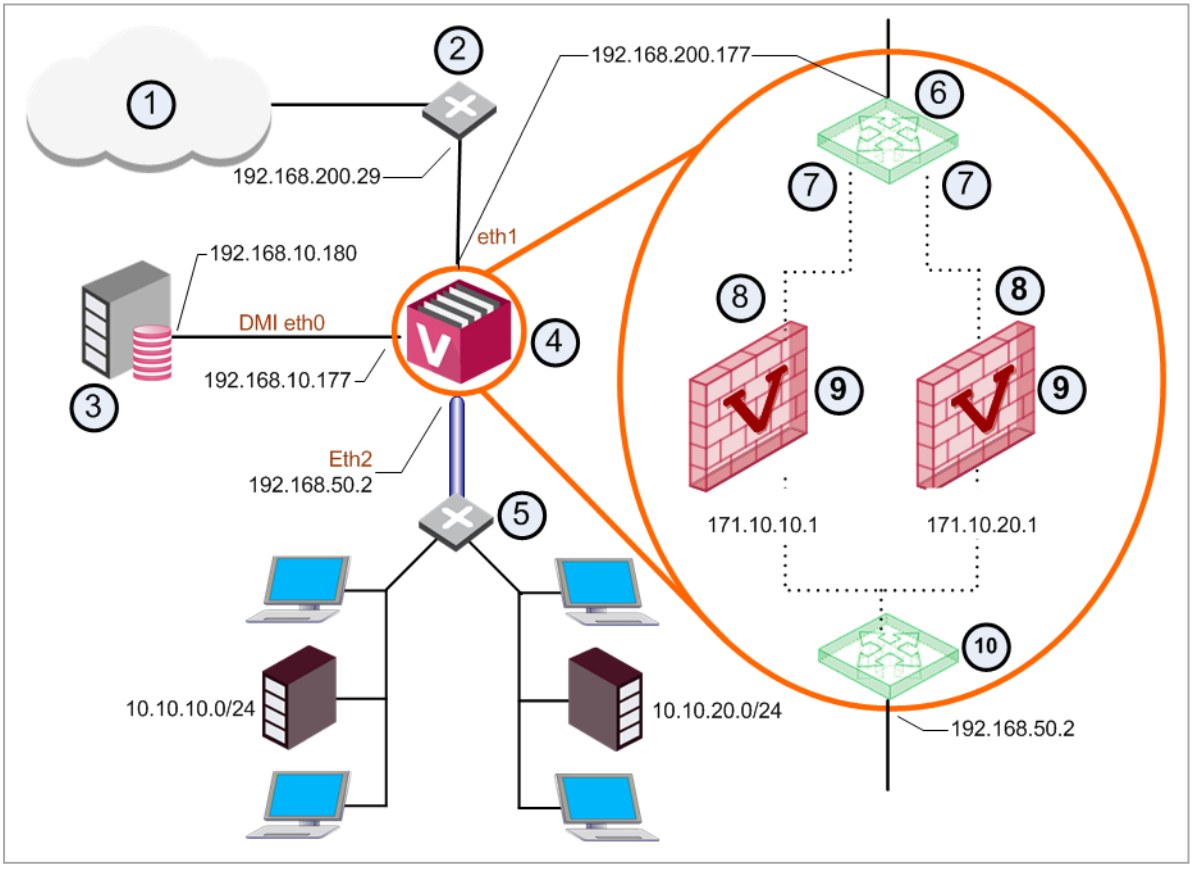
Introduction

Source-based routing directs traffic to a specific destination based on the source IP address or a combination of the source and destination IP addresses.

Rules defining Source-based routing take precedence over ordinary destination-based routing rules.

This section describes how to configure sourced-based routing rules when working in a VSX environment.

The procedures for defining source-based rules are the same for Virtual Routers in both VSX Gateways and VSX Clusters.



Item	Description		Item	Description
1	Internet		8	Wrp Unnumbered interface
2	Router		9	Virtual Systems
3	Security Management Server		10	Internal Virtual Router
4	VSX Gateway		-----	VLAN Interface
5	Switch		———	VLAN Truck
6	External Virtual Router		.....	Warp link
7	wrpj			

Defining Source-Based Routing Rules

Define Source-based Routing rules in the **Topology** page of the Virtual Router definition window.

To define source-based routing rules:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual Router.
2. From the **Gateways & Servers** view or **Object Explorer**, right-click the Virtual Router object and select **Edit**.

   The **General Properties** window opens.
3. From the left navigation tree, select **Topology**.
4. Click **Advanced Routing**.

   The **Advanced Routing Rules** window opens.
5. Click **Add** to define a new rule. or select an existing rule and click **Edit** to change it.

   The **Add/Edit Route Rule** window opens.
6. Define these settings:
   - **Source IP Address and Net Mask**
   - **Destination IP Address and Net Mask**
   - **Next Hop Gateway**
7. Click **OK**.

CoreXL for Virtual Systems

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.

Introduction

CoreXL creates multiple Firewall instances that are, in reality, independent firewalls. You can use CoreXL to increase the performance of the VSX Gateway with multiple CPU cores. You can also assign each CoreXL Firewall instance to a group of CPU cores with the "`fw ctl affinity`" command.

You configure CoreXL Firewall instances differently for the VSX Gateway (VS0) than for other Virtual Systems.

- **VSX Gateway** - Use the CLI to configure the number of CoreXL Firewall instances.
- **Other Virtual Systems** - Use SmartConsole to configure the number of CoreXL Firewall instances.

You can configure several CoreXL Firewall instances for each Virtual System. When you change the number of CoreXL Firewall instances on a Virtual System, there is some downtime for that Virtual System.

Important:

- Each CoreXL Firewall instance you create uses additional system memory. A Virtual System with five CoreXL Firewall instances would use approximately the same amount of memory as five separate Virtual Systems.
- The number of IPv6 instances cannot exceed the number of IPv4 CoreXL Firewall instances.

For more about configuring CoreXL, see the *R82 Performance Tuning Administration Guide* > Chapter "CoreXL".

Configuring CoreXL on a VSX Gateway

Important - Enabling CoreXL on VS0 is not recommended because of increased memory overhead and potential performance degradation. Most VSX deployments do not require more than a single Firewall instance for VS0 as its main purpose is managing the VSX Gateway.

Use the "`cpconfig`" command to configure CoreXL on the VSX Gateway (VS0).

The number of instances for the VSX Gateway is limited to the physical number of cores on the server or appliance.

To configure the number of instances on the VSX Gateway:

1. Connect to the command line on the VSX Gateway / each VSX Cluster Member.
2. Run:

   ```
   cpconfig
   ```

3. Select **Configure Check Point CoreXL**.
4. Make sure that CoreXL is enabled.
5. Configure the number of CoreXL Firewall instances.
6. Exit the `cpconfig` menu.

Note - It is not necessary to reboot the VSX Gateway after you configure CoreXL.

Configuring CoreXL on a Scalable Platform Security Group

Important - Enabling CoreXL on VS0 is not recommended because of increased memory overhead and potential performance degradation. Most VSX deployments do not require more than a single Firewall instance for VS0 as its main purpose is managing the Security Group.

To configure CoreXL on the Security Group (VS0):

- In Gaia gClish, use the "`cpconfig`" command.
- In the Expert mode, use the "`g_all cp_conf corexl`" command. See the *R82 CLI Reference Guide* > Chapter "CoreXL Commands" > Section "cp_conf corexl".

To configure the number of instances on the Security Group:

1. Connect to the command line on the Security Group.
2. Log in to Gaia gClish.

   If your default shell is the Expert mode, then run: `gclish`
3. Run:

   ```
   cpconfig
   ```
4. Select **Configure Check Point CoreXL**.
5. Make sure that CoreXL is enabled.
6. Configure the number of CoreXL Firewall instances.
7. Exit the `cpconfig` menu.

Note - It is not necessary to reboot the Security Group after you configure CoreXL.

Configuring CoreXL on Virtual Systems

Use SmartConsole to configure the number of CoreXL Firewall instances on the Virtual Systems.

In 64-bit Gaia, you can assign CoreXL Firewall instances up to the total number of CPU cores available on the Appliance. For example, if the appliance has 64 CPU cores, you can assign up to 64 CoreXL Firewall instances to a Virtual System..

You can assign the number of IPv6 CoreXL Firewall instances. It must be less or equal to the number of IPv4 CoreXL Firewall instances. The number of IPv6 CoreXL Firewall instances may be zero. IPv6 CoreXL Firewall instances are only enabled, if an IPv6 address is configured for that Virtual System.

Best practices:

1. We recommend that you use the number of CoreXL Firewall instances for each Virtual System according to the expected network traffic on the Virtual System. Configuring unnecessary CoreXL Firewall instances can have a negative impact on performance.
2. We recommend that you do not configure more CoreXL Firewall instances than the total number of physical CPU cores on the VSX Gateway.
3. After an upgrade to a higher major version:
   a. Connect to the command line on the VSX Gateway / each VSX Cluster Member / Security Group.
   b. Log in to Gaia Clish / Gaia gClish.
   c. Go to the context of VS0:
   ```
   set virtual-system 0
   ```
   d. Delete all existing CoreXL affinity settings and create the default CoreXL affinity settings during the next reboot:
   ```
   fw ctl affinity -vsx_factory_defaults
   ```
   e. Reboot:
      i. On a VSX Gateway / each VSX Cluster Member:
      ```
      reboot
      ```
      ii. On a Security Group:
      ```
      reboot -b <SGM IDs> -a
      ```

To configure CoreXL on a Virtual System:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual System.
2. From the **Gateways & Servers** view or **Object Explorer**, double-click the Virtual System object.

   The **Virtual System General Properties** window opens.
3. From the left navigation tree, select **CoreXL**.
4. Select the number of CoreXL Firewall instances for the Virtual System.
5. Click **OK**.
6. Install the Access Control Policy on the Virtual System object.

Dynamic Routing for Virtual Devices

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.
- Virtual Routers are not supported (Known Limitation 01413513).

This section presents procedures for configuring dynamic routing for Virtual Systems and Virtual Routers. The Virtual Devices can use dynamic routing protocols to communicate and distribute routes amongst themselves and with external routers and other devices. VSX uses the Gaia routing daemon (`routed`).

You can configure dynamic routing for each of these Virtual Devices:

- Virtual System
- Virtual Router

Each of these Virtual Devices has its own dynamic routing instance and configuration file. Use the same procedures to configure the dynamic routing protocols for Warp Links as regular interfaces. You can also configure dynamic routing separately on each VSX Cluster Member.

Important:

- You must configure all static routes only in SmartConsole in the applicable Virtual Device object.
- In a Cluster, you must configure all the Cluster Members in the same way.

To configure dynamic routing for a Virtual Device:

1. Connect to the command line on the VSX Gateway / each VSX Cluster Member.
2. Log in to Gaia Clish.

   On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.
3. Change the context to the Virtual Device:

   ```
   set virtual-system <VSID>
   ```
4. Run the applicable commands to configure the dynamic routing daemon for the Virtual Device.

   For dynamic routing syntax, see the *R82 Gaia Advanced Routing Administration Guide*.
5. Save the changes:

```
save config
```

Working with Interface Definitions

All VSX Gateways and Virtual Routers and Virtual Switches contain at least one interface definition.

Typically, you define the interfaces during the process of configuring the topology for a given object.

Warp interfaces, however, are created automatically based on Virtual Device definitions and their topology.

You cannot modify or delete a Warp interface.

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.
- Virtual Routers are not supported (Known Limitation 01413513).

Adding a New Interface

The procedure and options for defining an interface vary according to the object and the network topology.

Some properties and pages are not available for certain interface definitions.

To add a new interface:

1. Open the Virtual Device object.
2. From the navigation tree, click **Topology**.
3. From the **Interfaces** section, click **New** and select one of these options:
   - **Regular**
   - **Leads to Virtual Router**
   - **Leads to Virtual Switch**

   The **Interface Properties** window for the selected option opens.
4. Configure the applicable settings (see below).
5. Click **OK**.
6. Install the applicable Access Control Policy.

Configuring Connection Properties - General

The **General** tab defines the network connections associated with an interface.

One or more of these properties show, depending on the context.

- **Interface**: Select a physical interface from the list (physical interfaces only).
- **VLAN Tag**: VLAN tag associated with the defined interface.
- **IP Address** and **Net Mask**: IP address and net mask of the device associated with the interface.
- **Propagate route to adjacent Virtual Devices**: Enable to "advertise" the associated device to neighboring devices, thereby enabling connectivity between them. See *"VSX Routing Concepts" on page 70*.
- **MTU**: Maximum transmission unit size in bytes (default = 1,500).

Configuring Connections Leading to Virtual Routers and Virtual Switches

The **General** tab for interface connections leading to Virtual Routers or Virtual Switches contains connection properties specific to those Virtual Devices.

- **Leads to**: Select a Virtual Router or Virtual Switch.
- Enter the dedicated Virtual System**IP address** for this interface.
- The **Net Mask** property is always defined as **255.255.255.255** for IPv4 and **/128** for IPv6.
- **Propagate route to adjacent Virtual Devices**: Enable to "advertise" the associated device to neighboring devices, thereby enabling connectivity between them. See *"VSX Routing Concepts" on page 70*.
- **MTU**: Maximum transmission unit size in bytes (default = 1,500).

  The minimum and maximum MTU values are:

  - IPv6 MTU: 1280 - 16000
  - IPv4 MTU: 68 - 16000

Configuring Interface Topology

For some interface types, you can change some or all of these topology properties:

- **External**: The interface leads to external networks or to the Internet.
- **Internal**: The interface leads to internal networks or a DMZ:
  - **Not Defined**: All IP addresses behind this interface are considered a part of the internal network that connects to this interface.
  - **Network defined by the interface IP and Net Mask**: Only the network that directly connects to this internal interface.
  - **Network defined by routes**: The Virtual System dynamically calculates the topology for this interface.

    Note - To see this option, you must clear the option **Calculate topology automatically based on routing information** in the Virtual System object.
  - **Specific**: A specific object (a **Host**, a **Network**, a **Network Group**, an **Address Range**).
  - **Interface leads to DMZ**: Defines an interface as leading to a DMZ, which isolates a vulnerable, externally accessible resource from the rest of a protected, internal network.

Configuring Anti-Spoofing

Attackers can gain access to protected networks by falsifying or "spoofing" a trusted source IP address with high access privileges. It is important to configure Anti-Spoofing protection for VSX Gateways and Virtual Systems, including internal interfaces. You can configure Anti-Spoofing for an interface, provided that the topology for the interface is properly defined.

If you are using dynamic routing, disable the **Calculate topology automatically based on routing information** option, and manually configure the topology of the Virtual System.

To enable Anti-Spoofing for an interface:

1. From the **Topology** tab in the **Interface Properties** window, select **Perform Anti-Spoofing based on interface topology**.
2. Configure the tracking options.

Configuring Multicast Restrictions

IP multicast applications send one copy of each datagram (IP packet) and address it to a group of computers that wish to receive it. Multicast restrictions allow you to define rules that block outbound datagrams from specific multicast groups (IP address ranges). You can define multicast access restrictions for physical and Warp interfaces in a VSX environment.

	From	To
IPv4 (defined in RFC 1112)	`224.0.0.0`	`239.255.255.255`
IPv6	`ff00::`	`ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`

To enable multicast restrictions:

1. From the **Multicast Restrictions** tab in the **Interface Properties** window, select **Drop multicast packets by the following conditions**.
1. Select a restriction type:
   - **Drop multicast packets whose destination is in the list**
   - **Drop all multicast packets except those whose destination is in the list**
2. Click **Add**.

   The **Add Object** window opens.
3. Click **New > Multicast Address Range**.

   The **Multicast Address Range Properties** window opens.
4. Configure these settings:
   - **Name**
   - **Type**
   - If you selected **IP Address Range**, enter the **First** and **Last** IP addresses.
5. Click **OK**.
6. From the **Interface Properties** window, select a tracking option.
7. Click **OK** and close the **General Properties** window.
8. Add a rule to the Access Control Policy that allows traffic for the specified multicast groups.

Changing an Interface Definition

This section presents procedures for modifying existing interface definitions and related features.

Interfaces definitions are always associated with a VSX Gateway or a Virtual System definition.

To change an existing interface definition:

1. Double-click the interface in the **Interfaces** section.
2. In the **Interface Properties** window, define the interface properties.
3. Click **OK**.
4. Install the applicable Access Control Policy.

Deleting an Interface

To delete an interface:

1. From the **Topology** page, select the interface and click **Delete**.
2. Click **OK**.
3. Install the applicable Access Control Policy.

Working with Authentication

Authentication Schemes

Authentication schemes employ user names and passwords to identify valid users.

Some schemes are maintained locally, storing user names and passwords on the VSX Gateway, while others store authentication information on an external authentication server.

Some schemes, such as SecurID, are based on providing a one-time password.

For more information, see the *R82 Security Management Administration Guide* > Section *Configuring Authentication Methods for Users*.

Check Point Password

Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Security Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.

Operating System Password

OS Password is stored on the operating system of the computer on which the Security Gateway(for users) or Security Management Server (for administrators) is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server.

Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication.

The RADIUS protocol uses UDP to communicate with the gateway or the Security Management Server.

RADIUS servers and RADIUS server group objects are defined in SmartConsole.

TACACS

Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers.

TACACS is an external authentication method that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. For administrators, it is the Security Management Server that forwards the requests. The TACACS server, which stores user account information, authenticates users. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

SecurID

SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager (AM) and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the AM.

Using SecurID, the Security Gateway forwards authentication requests by remote users to the AM. For administrators, it is the Security Management Server that forwards the requests. The AM manages the database of RSA users and their assigned hard or soft tokens. The Security Gateway or the Security Management Server act as an AM agent and direct all access requests to the RSA AM for authentication. For additional information on agent configuration, refer to RSA Authentication Manager documentation.

There are no specific parameters required for the SecurID authentication method. Authentication requests can be sent over SDK-supported API or through REST API.

Configuring RADIUS or TACACS Authentication

These are the options to enable connectivity between Virtual Systems and a RADIUS or TACACS/TACACS+ server:

Option	Description
Shared configuration	All Virtual Systems connect to the RADIUS or TACACS/TACACS+ authentication servers through the VSX Gateway. This is the default option.
Private configuration	All Virtual Systems connect to the RADIUS or TACACS/TACACS+ authentication servers directly. The Virtual Systems use the Virtual System cluster IP address as the source address.

For Multi-Domain Server configurations, make sure that you configure the authentication settings on the Domain Management Server that manages the Virtual Systems.

Configuring Shared Authentication with RADIUS or TACACS

Configure shared authentication so that all the Virtual Systems on the VSX Gateway authenticate to the remote RADIUS or TACACS/TACACS+ server.

To configure shared authentication for RADIUS or TACACS/TACACS+:

1. Configure shared authentication on the Virtual Systems.
   a. Connect with SmartConsole to the Management Server.
   b. From the left navigation panel, click **Gateways & Servers**.
   c. Double-click the Virtual System object.

      The **Virtual Systems General Properties** window opens.
   d. From the navigation tree, select **Other** > **Authentication**.
   e. Make sure that **RADIUS** or **TACACS** and **Shared** are selected.
   f. Click **OK**.
   g. Install the policy on the Virtual Systems.

   Repeat these Steps for each Virtual System.
2. For a VSX Cluster:

   On the Management Server that manages this VSX Cluster, make sure that Hide NAT is disabled.

On Multi-Domain Server, work in the context of the Target Domain Management Server that manages the Virtual System.

a. Edit the applicable `table.def` file. See sk98339.

b. Make sure that the `no_hide_services_ports` parameter **contains** the UDP ports for RADIUS or TACACS, or the TCP ports for TACACS+.

The default ports are:

- RADIUS - 1645
- TACACS/TACACS+ - 49

Sample RADIUS parameter with Hide NAT *disabled*:

```
no_hide_services_ports = { <49, 6>, <49, 17>, <500,
17>, <259, 17>, <1701, 17>, <123, 17>, <1645, 17> };
```

c. Save the changes in the file and exit the editor.

d. In SmartConsole, install the policy on the Virtual Systems.

Configuring Private Authentication with RADIUS or TACACS

For private configurations, the active and standby Virtual Systems use the same encryption key to authenticate to the remote RADIUS or TACACS/TACACS+ server.

For High Availability configurations, make sure that the Active and Standby Virtual Systems on each VSX Cluster Member use the same VIP address.

To configure private authentication:

1. Configure private authentication on the VSX Gateway and the Virtual Systems.
   a. Connect with SmartConsole to the Management Server.
   b. From the left navigation panel, click **Gateways & Servers**.
   c. Double-click the VSX Gateway object.
      The **General Properties** view opens.
   d. From the navigation tree, select **Other** > **Legacy Authentication**.
   e. Make sure that **RADIUS** or **TACACS** are selected.
   f. Click **OK**.
   g. From SmartConsole, install the Access Control Policy on the Virtual System.

   Repeat these steps for each Virtual System.
2. For VSX Cluster:

On the Management Server that manages this VSX Cluster, make sure that Hide NAT is enabled.

For Multi-Domain Server, use the Domain Management Server that manages the Virtual System.

a. Edit the applicable `table.def` file (see sk98339) in a plain-text editor.

b. Make sure that the `no_hide_services_ports` parameter DOES NOT contain the UDP ports for RADIUS or TACACS, or the TCP ports for TACACS+.

   The default ports are:

   - RADIUS - 1645
   - TACACS/TACACS+ - 49

   Sample parameter with Hide NAT enabled:

```
no_hide_services_ports = { <500, 17>, <259, 17>, <1701,
17>, <123, 17> };
```

c. Save the changes in the file and exit the editor.

d. From SmartConsole, install the Access Control Policy on each Virtual System.

Configuring RSA SecurID Authentication

See the *R82 Security Management Administration Guide* > Chapter *Managing User and Administrator Accounts* > Section *Managing User Accounts* > Section *SecurID Authentication for Security Gateway*.

These are the options to enable connectivity between Virtual Systems and a SecurID ACE/Server (RSA Authentication Manager):

Option	Description
Shared configuration	All Virtual Systems on the VSX Gateway / VSX Cluster Member use the same encryption key file "`sdconf.rec`" to authenticate to the remote SecurID ACE/Server (RSA Authentication Manager). In a VSX Cluster, each VSX Cluster Member uses a different encryption key file "`sdconf.rec`" and node secret file "`securid`". For the MIP (Member IP) address, use the IP address of a VSX Gateway / VSX Cluster Member interface that connects to the SecurID ACE/Server (RSA Authentication Manager).

Option	Description
Private configuration	Each Virtual System uses unique encryption key file "`sdconf.rec`" and node secret file "`securid`" to authenticate to the remote SecurID ACE/Server (RSA Authentication Manager). On a VSX Gateway - for the MIP (Member IP) address, use the IP address of the Virtual System interface that connects to the SecurID ACE/Server (RSA Authentication Manager). On a VSX Cluster - for the MIP (Member IP) address, use the VIP (Virtual IP) address of the Virtual System interface that connects to the SecurID ACE/Server (RSA Authentication Manager).

On a Multi-Domain Server, make sure that you configure the authentication settings on the Domain Management Server that manages the Virtual Systems.

Configuring Shared Authentication with SecurID

Part 1 - On the SecurID ACE/Server (RSA Authentication Manager), generate the "`sdconf.rec`" files:

On the SecurID ACE/Server (RSA Authentication Manager), generate the "`sdconf.rec`" file with the MIP of the VSX Gateway / each VSX Cluster Member.

For example, if a VSX Cluster has three VSX Cluster Members, and each VSX Cluster Member has five Virtual Systems, then generate three "`sdconf.rec`" files - one file for each VSX Cluster Member.

Part 2 - Configure the shared authentication for each Virtual System:

1. Configure shared authentication in each Virtual System object:
    a. Connect with SmartConsole to the Management Server.
    b. From the left navigation panel, click **Gateways & Servers**.
    c. Double-click the applicable Virtual System object.
    d. From the left navigation tree, select **Other**> **Legacy Authentication**.
    e. Select **SecurID** and **Shared**.
    f. Click **OK**.
    g. Install the Access Control policy on the Virtual System.
2. For each Virtual System, create the "`sdopts.rec`" file that contains the required MIP address.

a. Connect to the command line on the VSX Gateway / each VSX Cluster Member.

   On a Scalable Platform, connect to the Security Group.

b. Log in to the Expert mode..

c. Change the context to the Virtual System 0:

   - On a VSX Gateway / each VSX Cluster Member:

     ```
     vsenv 0
     ```

   - On a Scalable Platform:

     ```
     g_all vsenv 0
     ```

d. Create the "`/var/ace/sdopts.rec`" file:

   - On a VSX Gateway / each VSX Cluster Member:

     ```
     touch /var/ace/sdopts.rec
     ```

   - On a Scalable Platform:

     ```
     g_all touch /var/ace/sdopts.rec
     ```

e. Edit the "`/var/ace/sdopts.rec`" file:

   ```
   vi /var/ace/sdopts.rec
   ```

f. Add this line to the "`/var/ace/sdopts.rec`" file:

   ```
   CLIENT_IP=<IP Address of interface on VSX Gateway /
   each VSX Cluster Member>
   ```

g. Save the changes in the file and exit the editor.

h. On a Scalable Platform, copy the updated "`/var/ace/sdopts.rec`" file to all Security Group Members:

   ```
   asg_cp2blades /var/ace/sdopts.rec
   ```

i. Copy the "`/var/ace/sdopts.rec`" file to each Virtual System:

   i. Change the context to the Virtual System:

      - On a VSX Gateway / each VSX Cluster Member:

        ```
        vsenv <VSID>
        ```

      - On a Scalable Platform:

        ```
        g_all vsenv <VSID>
        ```

   ii. Copy the "`/var/ace/sdopts.rec`" file:

      - On a VSX Gateway / each VSX Cluster Member:

        ```
        cp -v /var/ace/sdopts.rec $FWDIR/conf/
        ```

      - On a Scalable Platform:

        ```
        g_all cp -v /var/ace/sdopts.rec $FWDIR/conf/
        ```

3. Copy the same encryption key file `sdconf.rec` from the SecurID ACE/Server (RSA Authentication Manager) to the required directory on the VSX Gateway / each VSX Cluster Member / Security Group:

   - For Virtual System 0, copy the "`sdconf.rec`" file to the "`/var/ace/`" directory on the VSX Gateway / each VSX Cluster Member / Security Group.

- For other Virtual Systems, copy the file to the "`$FWDIR/conf/`" directory in the context of each Virtual System:

  a. Copy the "`sdconf.rec`" file to some temporary directory on the VSX Gateway / each VSX Cluster Member / Security Group.

     For example: `/var/tmp/`

  b. On a Scalable Platform, copy the "`sdconf.rec`" file in the temporary directory to all Security Group Members:

     ```
     asg_cp2blades /var/tmp/sdconf.rec
     ```

  c. Change the context to the Virtual System:

     - On a VSX Gateway / each VSX Cluster Member:

       ```
       vsenv <VSID>
       ```

     - On a Scalable Platform:

       ```
       g_all vsenv <VSID>
       ```

  d. Copy the "`sdconf.rec`" file from the temporary directory to the "`$FWDIR/conf/`" directory in the context of each Virtual System

     - On a VSX Gateway / each VSX Cluster Member:

       ```
       cp -v /var/tmp/sdconf.rec $FWDIR/conf/
       ```

     - On a Scalable Platform:

       ```
       g_all cp -v /var/tmp/sdconf.rec $FWDIR/conf/
       ```

4. If this is a VSX Cluster, then configure the required settings for the Cluster Hide NAT for traffic on the UDP port 5500:

   a. Connect to the command line on the Management Server.

   b. Log in to the Expert mode.

c. Edit the applicable `table.def` file.

```
vi /Path/To/Required/table.def
```

For the exact path, see the section "**Location of 'table.def' Files on the Management Server**" in:

- *R82 Security Management Administration Guide* > Chapter "Managing Gateways" > Section "Configuring Implied Rules or Kernel Tables for Security Gateways".
- *R82 Multi-Domain Security Management Administration Guide* > Chapter "Configuring Implied Rules or Kernel Tables for Security Gateways"

d. Make sure the "`no_hide_services_ports`" parameter contains the correct ports:

- If the SecurID ACE/Server (RSA Authentication Manager) expects the connection from each VSX Cluster Member (and not from the VSX Cluster Virtual IP address), then the "`no_hide_services_ports`" parameter must **contain** the port 5500 and protocol 17 (`<5500, 17>`):

  Example:

```
no_hide_services_ports = { <500, 17>, <259, 17>,
<1701, 17>, <123, 17>, <5500, 17> };
```

- If the SecurID ACE/Server (RSA Authentication Manager) expects the connection from the VSX Cluster Virtual IP address, then the "`no_hide_services_ports`" parameter must **not** contain the port 5500 and protocol 17 (`<5500, 17>`):

  Example:

```
no_hide_services_ports = { <500, 17>, <259, 17>,
<1701, 17>, <123, 17> };
```

e. Save the changes in the file and exit the editor.

f. In SmartConsole, install the Access Control on the Virtual Systems.

Part 3 - Distribute the node secret to the Virtual Systems:

The first time a VSX Gateway / VSX Cluster Member connects to the SecurID ACE/Server (RSA Authentication Manager), the server sends the node secret file (`securid`) to that VSX Gateway. It is necessary to copy this node file to all Virtual Systems.

1. Authenticate to the VSX Gateway with a SecurID ACE/Server (RSA Authentication Manager) user account.

   The SecurID ACE/Server (RSA Authentication Manager) sends the node secret file "`securid`" to the VSX Gateway / VSX Cluster Member.

2. Search for the file called "`securid`":

   ```
   find /var/ace/ -name securid -type f
   ```

3. On a Scalable Platform, copy the "`securid`" file to all Security Group Members:

   ```
   asg_cp2blades /var/ace/securid
   ```

4. Copy the "`securid`" file to the "`$FWDIR/conf/`" directory in the context of each Virtual System:

   a. Change the context to the Virtual System:

      - On a VSX Gateway / each VSX Cluster Member:

        ```
        vsenv <VSID>
        ```

      - On a Scalable Platform:

        ```
        g_all vsenv <VSID>
        ```

   b. Copy the "`securid`" file to Virtual Systems:

      - On a VSX Gateway / each VSX Cluster Member:

        ```
        cp -v /var/ace/securid $FWDIR/conf/
        ```

      - On a Scalable Platform:

        ```
        g_all cp -v /var/ace/securid $FWDIR/conf/
        ```

5. If this is a VSX Cluster, then on each VSX Cluster Member:

   - Locate a Virtual System that is Active on that VSX Cluster Member and do the all the previous steps in this Part 3.
   - If there are no Virtual Systems in the Active state on that VSX Cluster Member, fail-over to the applicable VSX Cluster Member and then do the all the previous steps in this Part 3.

Configuring Private Authentication with SecurID

Part 1 - On the SecurID ACE/Server (RSA Authentication Manager), generate the "`sdconf.rec`" files:

On the SecurID ACE/Server (RSA Authentication Manager), generate the "`sdconf.rec`" file with the MIP of the Virtual System.

For example, if a VSX Cluster has three VSX Cluster Members, and each VSX Cluster Member has five Virtual Systems, then generate five "`sdconf.rec`" files - one file for each Virtual System.

Part 2 - Configure the private authentication for each Virtual System:

1. Configure shared authentication in each Virtual System object:
   a. Connect with SmartConsole to the Management Server.
   b. From the left navigation panel, click **Gateways & Servers**.
   c. Double-click the applicable Virtual System object.
   d. From the left navigation tree, select **Other**> **Legacy Authentication**.
   e. Select **SecurID** and **Private**.
   f. Click **OK**.
   g. Install the Access Control policy on the Virtual System.
2. For each Virtual System, create the "`sdopts.rec`" file that contains the required MIP address.
   a. Connect to the command line on the VSX Gateway / each VSX Cluster Member.

      On a Scalable Platform, connect to the Security Group.
   b. Log in to the Expert mode..
   c. Change the context to the Virtual System:
      - On a VSX Gateway / each VSX Cluster Member:

        ```
        vsenv <VSID>
        ```

      - On a Scalable Platform:

        ```
        g_all vsenv <VSID>
        ```

d. Create the "`$FWDIR/conf/sdopts.rec`" file:

```
touch $FWDIR/conf/sdopts.rec
```

e. Edit the "`$FWDIR/conf/sdopts.rec`" file:

```
vi $FWDIR/conf/sdopts.rec
```

f. Add this line to the "`$FWDIR/conf/sdopts.rec`" file:

```
CLIENT_IP=<IP Address of interface on Virtual System>
```

g. Save the changes in the file and exit the editor.

h. On a Scalable Platform, copy the updated "`$FWDIR/conf/sdopts.rec`" file to all Security Group Members:

```
asg_cp2blades $FWDIR/conf/sdopts.rec
```

3. Copy the unique encryption key file `sdconf.rec` from the SecurID ACE/Server (RSA Authentication Manager) to the "`$FWDIR/conf/`" directory in the context of the required Virtual System on the VSX Gateway / each VSX Cluster Member / Security Group:

   a. Copy the "`sdconf.rec`" file to some temporary directory on the VSX Gateway / each VSX Cluster Member / Security Group.

      For example: `/var/tmp/`

   b. On a Scalable Platform, copy the "`sdconf.rec`" file in the temporary directory to all Security Group Members:

```
asg_cp2blades /var/tmp/sdconf.rec
```

   c. Change the context to the required Virtual System:

      - On a VSX Gateway / each VSX Cluster Member:

```
vsenv <VSID>
```

      - On a Scalable Platform:

```
g_all vsenv <VSID>
```

d. Copy the "`sdconf.rec`" file from the temporary directory to the "`$FWDIR/conf/`" directory in the context of the required Virtual System

- On a VSX Gateway / each VSX Cluster Member:

```
cp -v /var/tmp/sdconf.rec $FWDIR/conf/
```

- On a Scalable Platform:

```
g_all cp -v /var/tmp/sdconf.rec $FWDIR/conf/
```

4. If this is a VSX Cluster, then configure the required settings for the Cluster Hide NAT for traffic on the UDP port 5500:

a. Connect to the command line on the Management Server.

b. Log in to the Expert mode.

c. Edit the applicable `table.def` file.

```
vi /Path/To/Required/table.def
```

For the exact path, see the section "**Location of 'table.def' Files on the Management Server**" in:

- *R82 Security Management Administration Guide* > Chapter "Managing Gateways" > Section "Configuring Implied Rules or Kernel Tables for Security Gateways".
- *R82 Multi-Domain Security Management Administration Guide* > Chapter "Configuring Implied Rules or Kernel Tables for Security Gateways"

d. Make sure the "no_hide_services_ports" parameter contains the correct ports:

- If the SecurID ACE/Server (RSA Authentication Manager) expects the connection from each Virtual System (and not from the Virtual System Virtual IP address), then the "no_hide_services_ports" parameter must **contain** the port 5500 and protocol 17 (<5500, 17>):

  Example:

```
no_hide_services_ports = { <500, 17>, <259, 17>,
<1701, 17>, <123, 17>, <5500, 17> };
```

- If the SecurID ACE/Server (RSA Authentication Manager) expects the connection from the Virtual System Virtual IP address, then the "no_hide_services_ports" parameter must **not** contain the port 5500 and protocol 17 (<5500, 17>):

  Example:

```
no_hide_services_ports = { <500, 17>, <259, 17>,
<1701, 17>, <123, 17> };
```

e. Save the changes in the file and exit the editor.

f. In SmartConsole, install the Access Control on the Virtual System.

Part 3 - Distribute the node secret to the Virtual Systems:

The first time a VSX Gateway / VSX Cluster Member connects to the SecurID ACE/Server (RSA Authentication Manager), the server sends the node secret file (securid) to that VSX Gateway. It is necessary to copy this node file to all Virtual Systems.

1. Authenticate to the VSX Gateway with a SecurID ACE/Server (RSA Authentication Manager) user account.

   The SecurID ACE/Server (RSA Authentication Manager) sends the node secret file "securid" to the VSX Gateway / VSX Cluster Member.

2. Search for the file called "securid":

```
find /var/ace/ -name securid -type f
```

3. On a Scalable Platform, copy the "securid" file to all Security Group Members:

```
asg_cp2blades /var/ace/securid
```

4. Copy the "securid" file to the "$FWDIR/conf/" directory in the context of each Virtual System:

a. Change the context to the Virtual System:

   - On a VSX Gateway / each VSX Cluster Member:

     ```
     vsenv <VSID>
     ```

   - On a Scalable Platform:

     ```
     g_all vsenv <VSID>
     ```

b. Copy the "`securid`" file to Virtual Systems:

   - On a VSX Gateway / each VSX Cluster Member:

     ```
     cp -v /var/ace/securid $FWDIR/conf/
     ```

   - On a Scalable Platform:

     ```
     g_all cp -v /var/ace/securid $FWDIR/conf/
     ```

5. If this is a VSX Cluster, then on each VSX Cluster Member:

   - Locate a Virtual System that is Active on that VSX Cluster Member and do the all the previous steps in this Part 3.
   - If there are no Virtual Systems in the Active state on that VSX Cluster Member, fail-over to the applicable VSX Cluster Member and then do the all the previous steps in this Part 3.

Tracking the Status of VSX Objects

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.

Use the SmartConsole **Logs & Events** features to show the status of all Security Gateways, VSX Gateways and other Virtual Devices.

The **Overall** status of a Virtual Device is the most serious status of its Software Blades.

For example, if all the **Software Blades** statuses are **OK** except for the SmartEvent blade, which has a **Problem** status, then the **Overall** status will be **Problem**.

Status Icon	Description
OK	The VSX Gateway and all its Software Blades are working properly.
Attention	At least one Software Blade has a minor issue, but the VSX Gateway works.
Problem	At least one Software Blade reported a malfunction, or an enabled Software Blade is not installed.
Waiting	SmartView Monitor is waiting for the Security Management Server to send data from Security Gateways.
Disconnected	Cannot reach the Security Gateway.
Untrusted	Cannot make Secure Internal Communication between the Security Management Server and the VSX Gateway.

Working with Network Address Translation (NAT)

Note - In Security Groups in Maestro and Scalable Chassis:

- The term VSX Gateway means a Security Group in the VSX mode.
- Some VSX features have a limited or no support.
- Virtual Routers are not supported (Known Limitation 01413513).

This section describes the process for using Network Address Translation (NAT) in a VSX deployment.

The procedures described in this section assume that the reader is familiar with NAT concepts and their implementation in Check Point products.

For more about NAT, see the *R82 Security Management Administration Guide* - Section *Configuring NAT Policy*.

VSX supports NAT for Virtual Systems much in the same manner as a physical Security Gateway. When a NAT enabled (Static or Hide) Virtual System connects to a Virtual Router, the translated routes are automatically forwarded to the appropriate Virtual Router.

Configure NAT using the **NAT** page in the **Virtual System** window. Hide or Static NAT addresses configured in this manner are automatically forwarded to the Virtual Router to which the Virtual System is connected. Alternatively, you can manually add NAT routes on the **Topology** page in the **Virtual Router** window.

To configure NAT for a Virtual System on a VSX Gateway:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server / Target 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 navigation tree, click **NAT** > **Advanced**. The **Advanced** page opens.
5	Select **Add Automatic Address Translation**.

Step	Instructions
6	Select the **Translation method**. ■ **Hide** - Hide NAT only allows connections originating from the internal network. Internal hosts can access internal destinations, the Internet and other external networks. External sources cannot initiate a connection to internal network addresses. Select one of these options: • **Hide behind Gateway** - Hides the real address behind the VSX Gateway external interface address. This is equivalent to hiding behind the address `0.0.0.0` for IPv4, or `::` for IPv6. • **Hide behind IP Address** - Hides the real address behind a virtual IP address, which is a routable, public IP address that does not belongs to any real machine. ■ **Static** - Static NAT translates each private address to a corresponding public address. Enter the static IP address.
7	From the **Install on Gateway** list, select the VSX Gateway.
8	Click **OK**.
9	Install the Access Control Policy on this Virtual System.

To configure NAT for a Virtual System on a VSX Cluster:

Use case - Perform Hide NAT on traffic a Virtual System itself generates in a VSX Cluster, so that the Virtual System could connect to external resources (for example, update Anti-Bot signatures from the Check Point cloud).

Step	Instructions
1	Connect to the command line on each VSX Cluster Member.
2	Log in to the Expert mode.
3	Switch to the context of the applicable Virtual System: `[Expert@HostName:0]# vsenv <VSID>`

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>4</td><td>Get the Funny IP address of the applicable Virtual System interface, through which the applicable traffic goes out.
Note - Funny IP address is the IP address that belongs to cluster's internal communications network (open the VSX Cluster object properties and go to the "Cluster Members" pane).
Run one of these commands:
<code>[Expert@HostName:<<i>VSID</i>>]# fw getifs</code>
<code>[Expert@HostName:<<i>VSID</i>>]# \ifconfig</code>
Write down the Funny IP address.</td></tr>
<tr><td>5</td><td>Connect with SmartConsole to the Security Management Server / Target Domain Management Server that manages this Virtual System.</td></tr>
<tr><td>6</td><td>From the left navigation panel, click Gateways & Servers.</td></tr>
<tr><td>7</td><td>Create a new Node Host object and assign to it the Funny IP address you wrote down in Step 4.</td></tr>
<tr><td>8</td><td>Create a new Node Host object and assign to it the NATed IP address.</td></tr>
<tr><td>9</td><td>From the left navigation panel, click Security Policies.</td></tr>
<tr><td>10</td><td>In the Access Control > NAT policy, create the applicable NAT rule to hide the traffic from the Virtual System behind the NATed IP address:
<table>
<tr><th>Original Source</th><th>Original Destination</th><th>Original Services</th><th>Translated Source</th><th>Translated Destination</th><th>Translated Services</th><th>Install On</th></tr>
<tr><td>Must be a Node Host object with the Funny IP address of the Virtual System</td><td><code>Any</code></td><td><code>Any</code></td><td>Must be a Node Host object with the NATed IP address of the Virtual System</td><td><code>= Original</code></td><td><code>= Original</code></td><td><code>Policy Targets</code> or the Virtual System object</td></tr>
</table></td></tr>
<tr><td>11</td><td>Install the Access Control Policy on this Virtual System.</td></tr>
</table>

Configuring Application Control or URL Filtering on VSX

This section contains the instructions to enable Application Control and URL Filtering Software Blades on Virtual Systems.

For more information, see sk106496 and sk79700.

Important:

- Make sure the routing, DNS, and proxy settings for the VSX Gateway or VSX Cluster Members (VS0) are configured correctly.
- Do **not** enable these Software Blades in the VSX Gateway or VSX Cluster object.
- Make the VSX Gateway or VSX Cluster Members can connect to the Internet. Virtual Systems get updates through the VSX Gateway or VSX Cluster Members (VS0).

To enable Application Control and URL Filtering on Virtual Systems:

Step	Instructions
1	If applicable, configure proxy settings for the VSX Gateway or VSX Cluster (VS0), or the Virtual Systems (or both) in SmartConsole: a. From the left navigation panel, click **Gateways & Servers**. b. Double-click the VSX Gateway object (or the applicable Virtual System object). c. From the navigation tree, click **Topology** > **Proxy**. d. Configure the proxy settings. e. Click **OK**
2	Enable **Application Control** or **URL Filtering** on the applicable Virtual Systems: a. Double-click the applicable Virtual System object. b. From the navigation tree, click **General Properties**. c. On the **Network Security** tab, select any or all of these Software Blades: ■ Application Control ■ URL Filtering d. From the navigation tree, click and configure the Software Blades you enabled. e. Click **OK**.
3	Configure the Access Control policies for the applicable Virtual Systems.
4	Install the Access Control policies on the applicable Virtual Systems.

For more about Application & URL Filtering, see the *R82 Security Management Administration Guide*.

For more information about these Software Blades on VSX Gateway, see sk106496 and sk79700.

Configuring Threat Prevention on VSX

This section contains the instructions to enable Threat Prevention Software Blades on VSX Virtual Systems.

For more information, see sk106496 and sk79700.

To enable Anti-Bot, Anti-Virus, or IPSon Virtual Systems

Important:

- Make sure the routing, DNS, and proxy settings for the VSX Gateway or VSX Cluster Members (VS0) are configured correctly.
- You must enable and configure the Software Blades in these objects:
  - VSX Gateway or VSX Cluster (because VS0 handles contract validation for all Virtual Systems).
  - Applicable Virtual Systems.
- Make sure the VSX Gateway or VSX Cluster and the applicable Virtual Systems can connect to the Internet.
  Virtual Systems get updates through the VSX Gateway or VSX Cluster (VS0).
  If the VSX Gateway or VSX Cluster fails to connect, each Virtual System uses its proxy settings to get the updates from the Internet.

Step	Instructions
1	If applicable, configure proxy settings for the VSX Gateway or VSX Cluster (VS0) or the Virtual Systems (or both) in SmartConsole: a. From the left navigation panel, click **Gateways & Servers**. b. Double-click the VSX Gateway or VSX Cluster object (or the applicable Virtual System object). c. From the navigation tree, click **Topology** > **Proxy**. d. Configure the proxy settings. e. Click **OK**

Step	Instructions
2	Enable the Software Blade on the VSX Gateway or VSX Cluster (VS0): a. Double-click the applicable VSX Gateway or VSX Cluster object. b. From the navigation tree, click **General Properties**. c. On the **Threat Prevention** tab, select any or all of these Software Blades: ▪ Anti-Bot ▪ Anti-Virus ▪ IPS When you enable these Software Blades, the **First Time Activation** window opens. You must select: ▪ **According to the policy** ▪ **Detect only** d. From the navigation tree, click and configure the Software Blades you enabled. e. Click **OK**.
3	Enable the Software Blade on the applicable Virtual Systems: a. Expand the VSX Gateway or VSX Cluster object and double-click the applicable Virtual System object. b. From the navigation tree, click **General Properties**. c. On the **Threat Prevention** tab, select any or all of these Software Blades (the same you selected in the VSX Gateway or VSX Cluster object): ▪ Anti-Bot ▪ Anti-Virus ▪ IPS When you enable these Software Blades, the **First Time Activation** window opens. You must select: ▪ **According to the policy** ▪ **Detect only** d. From the navigation tree, click and configure the Software Blades you enabled. e. Click **OK**.
4	Configure the Threat Prevention policies for: ▪ The VSX Gateway or VSX Cluster (VS0). ▪ The applicable Virtual Systems.
5	Install the default VSX policy on the VSX Gateway or VSX Cluster. This policy is called: *<Name of VSX Gateway or VSX Cluster Object>*_VSX

Step	Instructions
6	Install the Threat Prevention policy: ■ On the VSX Gateway or VSX Cluster (VS0). ■ On the applicable Virtual Systems (and Access Control Policy, if needed).

To enable Threat Emulationon Virtual Systems

Important:

- Make sure the routing, DNS, and proxy settings for the VSX Gateway or VSX Cluster Members (VS0) are configured correctly.
- Do **not** enable the Threat Emulation Software Blade in the VSX Gateway or VSX Cluster object, because it does not participate in the Threat Emulation process.

Step	Instructions
1	If applicable, configure proxy settings for the VSX Gateway or VSX Cluster (VS0), or the Virtual Systems (or both) in SmartConsole: a. From the left navigation panel, click **Gateways & Servers**. b. Double-click the VSX Gateway or VSX Cluster object (or the applicable Virtual System object). c. From the navigation tree, click **Topology** > **Proxy**. d. Configure the proxy settings. e. Click **OK**
2	Enable **Threat Emulation** on the applicable Virtual Systems: a. Expand the VSX Gateway or VSX Cluster object and double-click the applicable Virtual System object. b. From the navigation tree, click **General Properties**. c. On the **Custom Threat Prevention** tab, select **SandBlast Threat Emulation**. The **Threat Emulation First Time Activation Wizard** opens. d. Configure the **Emulation Location** and click **Next**. e. Configure the settings on the **Activate Threat Extraction** page and click **Next**. f. In the **Summary** window, click **Finish**. g. From the navigation tree, click and configure the Software Blades you enabled. h. Click **OK**.

Step	Instructions
3	Configure the Threat Prevention policies for the applicable Virtual Systems.
4	Install the Threat Prevention policy on the applicable Virtual Systems (and Access Control Policy, if needed).

To enable Threat Extraction on Virtual Systems

Important:

- Make sure the routing, DNS, and proxy settings for the VSX Gateway or VSX Cluster Members (VS0) are configured correctly.
- Enable the Threat Extraction Software Blade in the VSX Gateway or VSX Cluster object.

Step	Instructions
1	If applicable, configure proxy settings for the VSX Gateway or VSX Cluster (VS0) or the Virtual Systems (or both) in SmartConsole: 1. From the left navigation panel, click **Gateways & Servers**. 2. Double-click the VSX Gateway or VSX Cluster object (or the applicable Virtual System object). 3. From the navigation tree, click **Topology** > **Proxy**. 4. Configure the proxy settings. 5. Click **OK**
2	Enable **Threat Extraction** on the applicable Virtual Systems: 1. Expand the VSX Gateway or VSX Cluster object and double-click the applicable Virtual System object. 2. From the navigation tree, click **General Properties**. 3. On the **Threat Prevention** tab, select **SandBlast Threat Extraction**. 4. Click **OK**.
3	Optional: When you enable Threat Extraction, support for web traffic over the HTTP and HTTPS protocol is enabled automatically. For Threat Extraction to scan e-mail attachments as well, configure the Security Gateway as a Mail Transfer Agent (MTA) (see the *R82 Threat Prevention Administration Guide* > Chapter *Mail Transfer Agent*.
4	Configure the Threat Prevention policies for: - The VSX Gateway or VSX Cluster (VS0). - The applicable Virtual Systems.

Step	Instructions
5	Install the default VSX policy on the VSX Gateway or VSX Cluster. This policy is called: *<Name of VSX Gateway or VSX Cluster Object>*_VSX
6	Install the Threat Prevention policy: ■ On the VSX Gateway or VSX Cluster (VS0). ■ On the applicable Virtual Systems (and Access Control Policy, if needed).

Licensing VSX

Check Point software is activated with a license key. To obtain a license key, register the certificate key (that appears on the back of the software media pack) with the Check Point User Center. The certificate key is used to generate a license key for the products that you are either evaluating or purchasing. To purchase the required Check Point products, contact your reseller.

VSX Licenses

Each VSX Gateway or VSX Cluster Member requires its own license, bound to the VSX Gateway or VSX Cluster Member IP address. Each VSX Gateway or VSX Cluster license covers a predefined number of Virtual Systems (3, 10, 25, and 50), and these licenses (except for 3) are cumulative. The VSX licenses are applied in addition to the Security Gateway license (container and Software Blades).

Upgrading Licenses

Before upgrading a Security Gateway or Security Management Server to R82, you need to have a valid support contract that includes software upgrade and major releases registered to your Check Point User Center account. The Security Management Server stores the contract file and downloads it to Security Gateways during the upgrade. By verifying your status with the User Center, the contract file enables you to easily remain compliant with current Check Point licensing standards.

The Trial Period

When installing a Check Point product for the first time, users receive a 15 day trial period, during which the product is fully functional. Once the trial period expires, you must purchase and install the appropriate permanent product licenses. During the trial period, you can configure up to 25 Virtual Systems.

Using VSX with Multi-Domain Server

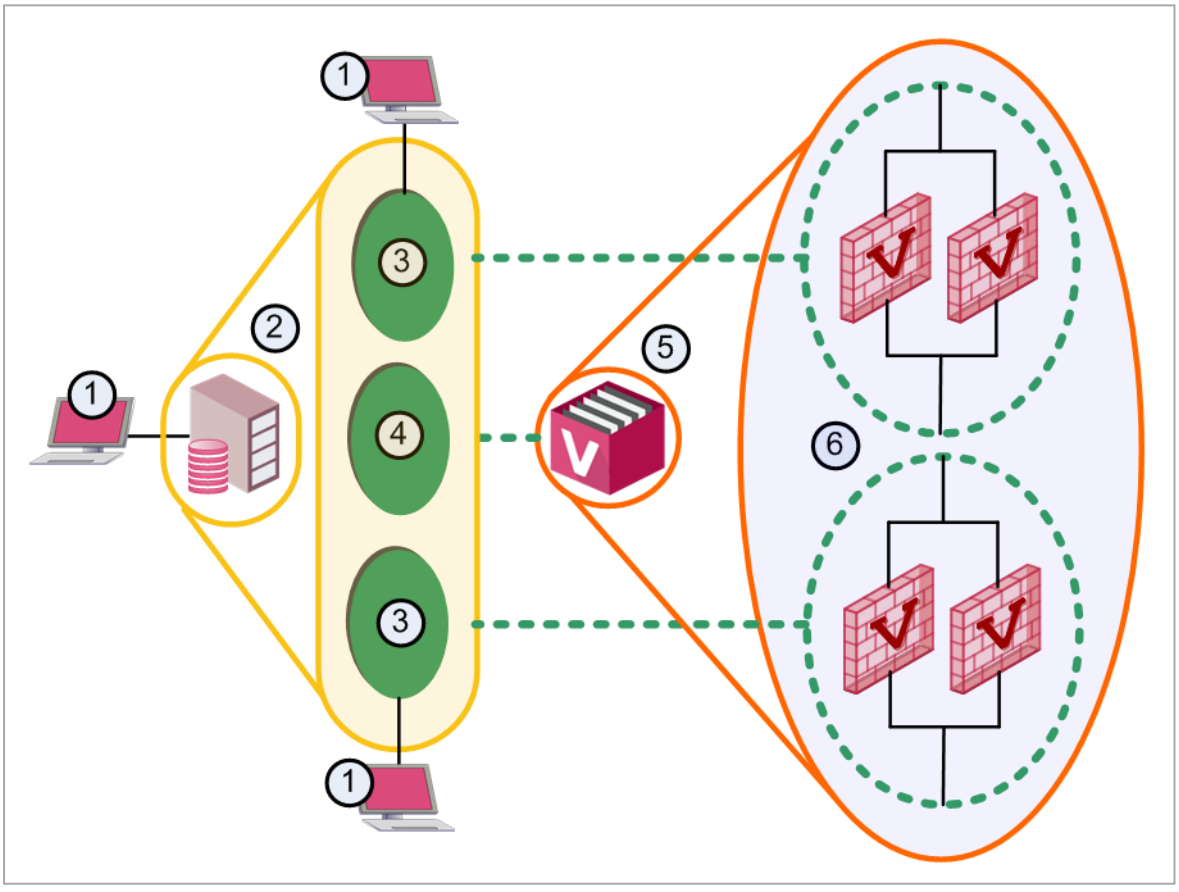
You can manage a VSX deployment using Multi-Domain Server.

Only procedures specific to VSX deployments are discussed.

This chapter assumes that you are familiar with the Multi-Domain Server product.

For more about Multi-Domain Server, see the *R82 Multi-Domain Security Management Administration Guide*.

Check Point Multi-Domain Server is a centralized security management solution that addresses the unique requirements of service providers and large enterprises. By using Multi-Domain Server, administrators can centrally manage multiple independent networks, often belonging to different Domains, divisions, or branches.



Item	Description
1	SmartConsole
2	Multi-Domain Server

Item	Description
3	Domain Management Server
4	Main Domain Management Server
5	VSX Gateway
6	Virtual Systems in Domain Management Servers

The **Multi-Domain Server** is a central Management Server that hosts the network management and security policy databases for these networks. Each independent domain is represented by a **Domain**, which provides the full functionality of a Security Gateway. Each Domain Management Server can host Virtual Systems, Virtual Routers and Virtual Switches as well as physical Check Point Security Gateways.

The Domain Management Server that manages a VSX Gateway or cluster is known as a **Main Domain Management Server**. You can host multiple Gateways and/or clusters on one Multi-Domain Server. Virtual Systems belonging to a given Domain can be distributed among multiple VSX Gateways and clusters.

When connected to a Multi-Domain Server, SmartConsole offers a centralized management solution for Domains, Domain Management Servers and the Multi-Domain Server environment. Each Domain Management Server uses its own instance of SmartConsole, which is accessible only via the Multi-Domain Server, to provision its Virtual Devices and physical Gateways, as well as to manage their Security Policies.

VSX Provisioning

The procedures for provisioning and configuring VSX Gateways, clusters and Virtual Devices using the Multi-Domain Server model are essentially the same as described for the Security Gateway management model.

The most important difference is that you must first create and configure each Domain and its associated Domain Management Server objects using the SmartConsole connected to a Multi-Domain Server.

Each Domain Management Server is the functional equivalent of one VSX Gateway.

You connect to each Domain Management Server with SmartConsole to work with network objects, security policies and other objects for that VSX Gateway.

This is the basic workflow for provisioning a VSX environment in a Multi-Domain Server deployment:

1. Define and configure Multi-Domain Server and Multi-Domain Log Server as applicable for your deployment.
2. Create and configure a Domain and Domain Management Server for each VSX Gateway and/or VSX Cluster.
3. With SmartConsole, connect to the Domain Management Server to create and configure the VSX Gateway and/or VSX Cluster objects.

   See *"Working with VSX Gateways" on page 104* and *"Working with VSX Clusters" on page 191*.

   Configure the default security policy for these objects as necessary.
4. Define individual Domains and Domain Management Servers as required for your deployment.
5. Create and configure Virtual Systems and other Virtual Devices for each Domain in the SmartConsole connected to that Domain.

   See *"Working with Virtual Systems" on page 109*, *"Working with Virtual Switches" on page 128*, and *"Working with Virtual Routers" on page 132*.

Defining Multi-Domain Servers

This section briefly presents the procedures for installing and deploying Multi-Domain Server machines in a VSX / Multi-Domain Server environment.

See the *R82 Multi-Domain Security Management Administration Guide* for conceptual information and detailed procedures for configuring Multi-Domain Servers and Domain Management Servers.

When working with Management High Availability, define at least two Multi-Domain Server machines.

You can also use multiple Multi-Domain Server machines to efficiently distribute management traffic (management Load Sharing) with more than one Domain Management Server for each Domain. For a Load Sharing deployment, define a Domain Management Server for each Multi-Domain Server.

Working with Virtual Devices on a Multi-Domain Server

When working with Virtual Devices in Multi-Domain Server, you must use the applicable Domain Management Server SmartConsole.

Otherwise, the configuration procedures are the same to those for a Security Management Server.

Multi-Domain Server treats Virtual Devices in the same way as physical devices.

You can add as many Virtual Systems to Domain Management Servers as your license permits.

Virtual Systems added to a Domain Management Server do not have to reside on the same VSX Gateway or cluster.

Adding a Virtual System to a Domain Management Server

To add a new Virtual System to a Domain Management Server:

1. Launch SmartConsole from the appropriate Domain Management Server.
2. Create and configure the Virtual System (see *"Working with Virtual Systems" on page 109*).
3. Define and install a security policy.

Adding Virtual Routers and Virtual Switches to a Domain Management Server

Note - Security Groups in Maestro and Scalable Chassis do not support Virtual Routers (Known Limitation 01413513).

To add Virtual Routers and Virtual Switches to a Domain Management Server:

1. Launch SmartConsole from the appropriate Domain Management Server.
2. Create and configure Virtual Routers (see *"Working with Virtual Routers" on page 132*) and Virtual Switches (see *"Working with Virtual Switches" on page 128*) as required.

Configuring VSX Clusters

Important - This chapter does not apply to Scalable Platforms (Maestro and Chassis).

This chapter presents a conceptual overview of VSX Cluster deployments, with emphasis on clustering features and their application.

It assumes you are familiar with network cluster applications and environments, particularly ClusterXL.

For more about Check Point ClusterXL features and functionality, see the *R82 ClusterXL Administration Guide*

VSX Cluster Overview

VSX Clusters provide redundancy and load sharing features for Virtual Systems and other Virtual Devices.

A VSX Cluster consists of two or more identical, interconnected VSX Gateways that ensure continuous data synchronization.

The advantages of using clusters in a VSX environment include:

- Transparent failover in case of VSX Cluster Member or Virtual System failure
- State synchronization ensures zero downtime for mission-critical environments
- Load Sharing maintains system throughput during peak demand
- Enhanced scalability for future traffic growth

VSX Cluster Modes:

Mode	Description
Virtual System Load Sharing (VSLS)	Ensures continuous operation by means of transparent VSX Cluster Member failover. Enhances system performance by distributing Active Virtual Systems amongst VSX Cluster Members. Efficiently balances network traffic load by distributing active Virtual Systems between VSX Cluster Members. All VSX Cluster Members and Virtual Systems are continuously synchronized. **Note** - This is the only mode available for a VSX Cluster that was installed as R81.10 or higher.

Mode	Description
High Availability	Ensures continuous operation by means of transparent VSX Cluster Member failover. All VSX Cluster Members and Virtual Systems function in an the Active/Standby mode and are continuously synchronized. **Note** - This mode is available only if you upgrade a VSX Cluster from R81 or lower to R82.

Physical Clusters

VSX Cluster is based on Check Point ClusterXL concepts. This section reviews these concepts, and then demonstrates how these principles apply to VSX virtualization.

In typical Security Gateway deployment, a cluster consists of two or more identical, interconnected physical Security Gateways that provide redundancy and/or Load Sharing. This cluster behaves as a single Security Gateway and is assigned its own IP address, which is known as its **Cluster IP** or **Virtual IP** address. This IP address is distinct from the physical IP addresses of its VSX Cluster Members, which are hidden from the networks connected to the cluster.

Traffic from external networks or the Internet directed to the internal networks arrives at the external cluster IP address. Depending on the clustering mode (High Availability or Load Sharing), a designated VSX Cluster Member receives the traffic and performs the required inspection. After inspection, traffic is either sent to its destination on the internal network, or dropped.

Internal networks send traffic destined for the Internet or external networks, to the cluster IP address. This traffic is processed by the designated VSX Cluster Member, inspected, and forwarded to its external destination.

Each member interface has a unique, physical IP addresses. These IP addresses, which are invisible to physical networks, are used for internal communication between VSX Cluster Members and the Management Server for such tasks as downloading Security Policies, sending logs and checking the status of individual VSX Cluster Members.

VSX Clusters

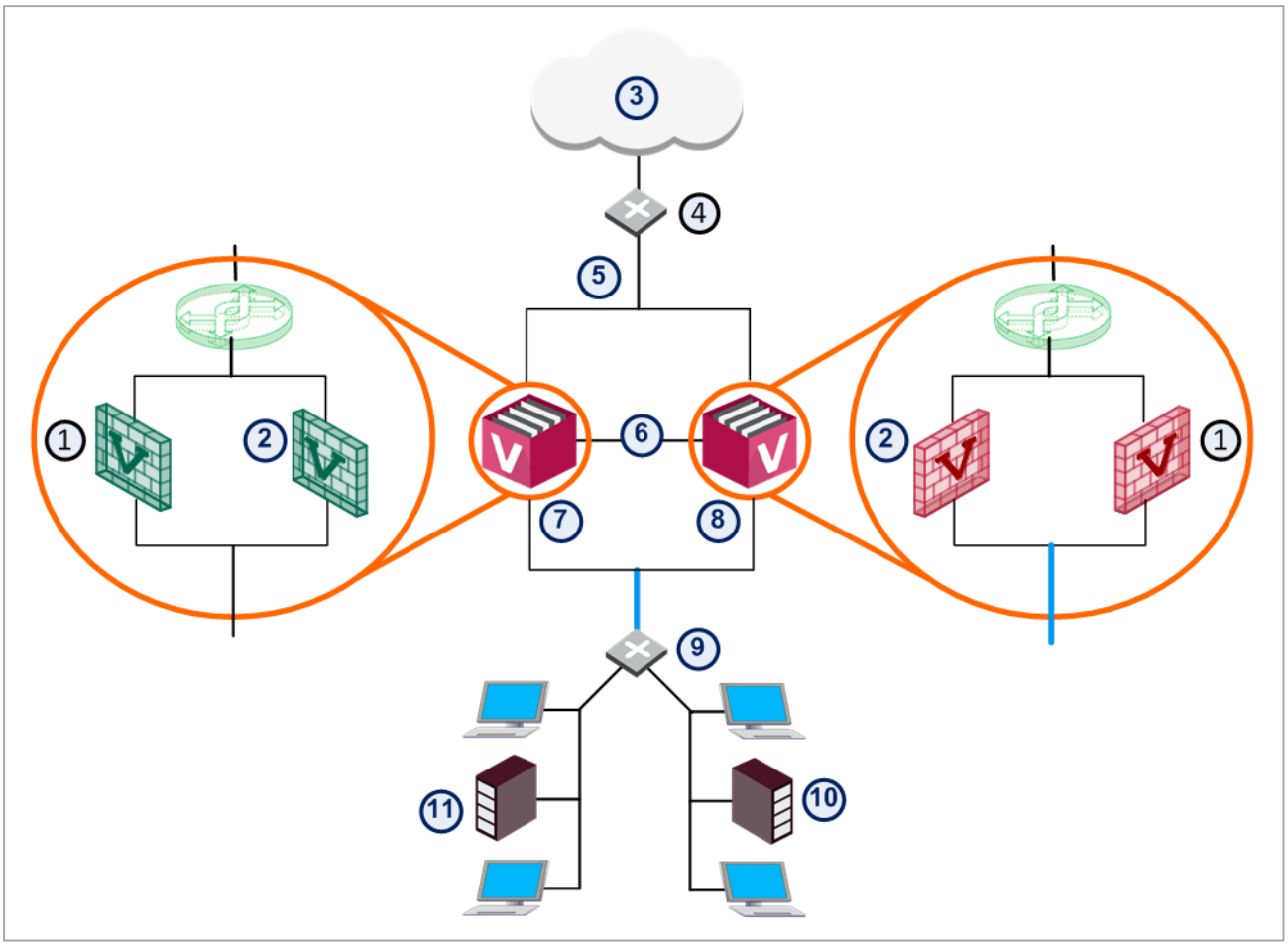
VSX Clusters, like their physical counterparts, connect two or more synchronized Gateways in such a way that if one fails, another immediately takes its place.

VSX Clusters are defined at two levels:

VSX ensures that Virtual Systems, Virtual Routers, Virtual Switches and their interfaces are provisioned and configured identically on each VSX Cluster Member.

The figure below shows that each VSX Cluster Member contains identical instances of each Virtual Device.

These identical instances are referred to as **peers**.



Item	Description		Item	Description
1	Virtual System 2		7	VSX Cluster Member 1
2	Virtual System 1		8	VSX Cluster Member 2
3	Internet		9	VLAN switch
4	Router		10	Network 2
5	External Cluster Interface		11	Network 1
6	Sync			VLAN Trunk

VSX provides the management functionality to support network and security virtualization, including:

- **Assigning virtual IP addresses**: Each Virtual Device interface requires its own virtual IP address.
- **State synchronization**: Virtual Device state tables are synchronized to peers on other VSX Cluster Members.

Planning a VSX Cluster Deployment

Important - This section does not apply to Scalable Platforms (Maestro and Chassis).

As with physical network deployments, advance planning is the key to successfully creating a working network.

IP address allocation for a VSX deployment requires particular attention.

This section takes you through the basics of IP address allocation for a VSX Cluster environment.

Your VSX Cluster configuration choices affect the number of IP addresses required, both public and private.

VSX Cluster Architecture

VSX IP address allocation is similar to physical networks.

Both real and virtual IP addresses are required for network connectivity (internal and external), management, and state synchronization.

VSX simplifies the IP address management task by automatically assigning IP addresses to Warp Links between Virtual Devices.

For example, Warp Links between a Virtual Router and its associated Virtual Systems are created automatically and assigned IP addresses without user intervention.

A VSX Cluster network has these components:

- Synchronization Network
- Internal Communications Network
- Virtual IP addresses

Synchronization Network

The synchronization network is a physical network that carries state synchronization data between VSX Cluster Members.

You configure the synchronization network during the initial VSX Cluster definition and can make changes as necessary when adding or removing VSX Cluster Members.

State Synchronization can be used ClusterXL deployments as well as other OPSEC-certified VSX solutions.

The synchronization network must be configured using unique IP addresses that are not used anywhere else in the enterprise network.

Internal Communication Network

The internal communication network is a virtual network that is required for ClusterXL environments, in addition to the synchronization network.

The internal communication network is invisible to external networks and lets VSX Cluster Members communicate and recognize the state of the environment.

VSX assigns an IP address to the internal communication network during the cluster creation process.

This eliminates the need to manually assign an IP address to each VSX Cluster Member:

IPv4 address: `192.168.196.0`, netmask: `255.255.252.0` (a range of four class C networks).

IPv6 address and netmask: `FD9A::1FFE:0:0:0/80`

You can modify the default IP address using the **Gateway Cluster Properties** > **Cluster Members** page of the VSX Cluster object, but only before creating Virtual Systems.

Once Virtual Systems have been created, the IP range of the internal communication network cannot be modified.

Note - To avoid overlapping IP addresses, before creating any Virtual Devices, make sure the default IP address range of the Internal Communication network is not used anywhere else in the external network.

Virtual IP Addresses

Cluster Virtual IP addresses are the only IP addresses visible to the external network.

The assigned cluster IP addresses must correspond to the directly-connected subnet and server as a valid next hop address.

These IP addresses are similar to virtual addresses configured across traditional cluster setups.

Working with VSX Clusters

Important - This section does not apply to Scalable Platforms (Maestro and Chassis).

Configuration Overview

You use SmartConsole for most of the basic cluster configurations.

Many cluster management procedures require the command line.

For example, you need the CLI to change the VSX Cluster definitions.

Creating VSX Clusters

This section describes how to create a new VSX Cluster using the **VSX Cluster Wizard**. The wizard guides you through the steps to configure a VSX Cluster.

After completing the VSX Cluster Wizard, you can modify most VSX Cluster and VSX Cluster Member properties directly from SmartConsole.

1. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages the VSX Cluster.
2. From the left navigation panel, click **Gateways & Servers**.
3. At the top, click **Objects** menu > **More object types > Network Object > Gateways and Servers > VSX > New Cluster**.

   The **VSX Cluster Wizard** > **General Properties** opens.

The VSX Cluster Wizard shows these pages:

Defining Cluster General Properties

The **Cluster General Properties** page contains basic properties for VSX Clusters:

- **VSX Cluster Name**: Unique, alphanumeric name for the cluster. The name cannot contain spaces or special characters except the underscore.
- **VSX Cluster IPv4 Address**: IPv4 address of the cluster.
- **VSX Cluster IPv6 Address**: IPv6 address of the cluster.
- **VSX Cluster Version**: VSX version to use for this cluster.
- **VSX Cluster Platform**: Platform type hosting the VSX Cluster Members:
  - To create a High Availability cluster, select **ClusterXL**.
  - To create a Load Sharing (VSLS) cluster, select **ClusterXL Virtual System Load Sharing**.

Note - All VSX Cluster Members must use the same type of platform, with the same specifications and configuration.

Adding VSX Cluster Member

The **VSX Cluster Members** window defines the members of the new cluster. You must define at least two VSX Cluster Members. You can add more members later.

1. In the **VSX Cluster Members** window, click **Add**.
2. The **Member Properties** window opens.
3. Enter the name and IP addresses for the VSX Cluster Member.

   Note: If you define an IPv6 IP address, you must also have an IPv4 address.
4. Enter and confirm the Activation Key to initialize the SIC trust between the VSX Cluster Member and the Management Server.

   Note - You defined this Activation Key during the First Time Configuration Wizard of the VSX Cluster Member.
5. Follow these steps for all VSX Cluster Members.
6. Click **Next** to continue.

Defining Cluster Interfaces

The **VSX Cluster Interfaces** window lets you define physical interfaces as VLAN Trunks.

The list shows all interfaces currently defined on the VSX Gateway or VSX Cluster object.

To configure a VLAN Trunk:

Select one or more interfaces to define them as VLAN Trunks. You can clear an interface to remove the VLAN Trunk assignment.

Important - You cannot define the management interface as a VLAN trunk. To use the management interface as a VLAN, you must define the VLAN on the VSX Gateway before you use SmartConsole to create the VSX Gateway object.

Configuring VSX Cluster Members

If you selected the custom configuration option, the **VSX Cluster Members** window appears.

In this window, you define the synchronization IP address for each VSX Cluster Member.

To configure the VSX Cluster Members:

1. Select the synchronization interface from the list.
2. Enter the synchronization interface addresses and net mask for each VSX Cluster Member.

To use a VLAN as a synchronization interface:

1. On each VSX Cluster Member, define the VLAN interface on the applicable physical interface.
2. In SmartConsole, create the VSX Cluster object.
3. On each VSX Cluster Member, set the value of the kernel parameter "`fwha_monitor_all_vlan`" to 1 in the `$FWDIR/boot/modules/fwken.conf` file. For more information, see sk92826 and *"Working with Kernel Parameters" on page 435*.

Cluster Management

The **VSX Gateway Management** page allows you to define several security policy rules that protect the cluster itself. This policy is installed automatically on the new VSX Cluster.

Note - This policy applies **only** to traffic destined for the cluster. This policy does not apply to traffic that is destined for Virtual Systems, other Virtual Devices, external networks, and internal networks.

The security policy consists of predefined rules covering the following services:

- **UDP**: SNMP requests
- **TCP**: SSH traffic
- **ICMP**: Echo-request (ping)
- **TCP**: HTTPS (secure HTTP) traffic

Configuring the Cluster Security Policy

1. **Allow**: Enable a rule to allow traffic for those services for which you wish to allow traffic. Clear a rule to block traffic. By default, all services are blocked.

   For example, you may wish to allow UDP `echo-request` traffic in order to be able to ping VSX Cluster Member from the Management Server.

2. **Source**: Click the arrow and select a **Source Object** from the list. The default value is ***Any**.

   Click **New Source Object** to define a new source.

   For more about Security Policies, see the *R82 Security Management Administration Guide*.

Completing the Wizard

1. Click **Next** to continue and then click **Finish** to complete the VSX Cluster wizard.

   It can take several minutes to complete. A message appears indicating successful or unsuccessful completion of the process.

   If the process ends unsuccessfully, click **View Report** to view the error messages.

   Refer to the troubleshooting steps for more information - *"VSX Diagnostics and Troubleshooting" on page 283*.

2. In SmartConsole, double-click the new VSX Cluster object.
3. Configure the applicable settings.
4. Click **OK**.

5. Install the Access Control Policy.
6. Install the Threat Prevention Policy.

Modifying a VSX Cluster Definition

In This Section:

General Properties 197
VSX Cluster Members 197
ClusterXL 198
Physical Interfaces 198
Synchronization 198
Topology 199
NAT 201
VSX Bridge Configuration 202
Changing the Cluster Management IP and/or Subnet 202
Changing the Internal Communication Network IP 203

Important - This section does not apply to Scalable Platforms (Maestro and Chassis).

After you create a cluster with the wizard, you can change the topology and other parameters in the **Cluster Members Properties** window. This window lets you configure many advanced features not available with the wizard.

To work with a VSX Cluster definition, double-click a cluster object in SmartConsole. The **VSX Cluster Properties** window opens.

You can define most cluster objects with SmartConsole. There are some features or properties that you must CLI commands to configure.

A brief explanation for each of the definition pages follows. More detailed explanations for features that are not specific to VSX (NAT, IPS, VPN, etc.) are available in the online help or in the applicable product documentation.

General Properties

See the **General Properties** page to view general properties and to activate Software Blades for use with this VSX Cluster.

You can modify the following properties:

- **Comment**: Free text comment that appears in the Object List and elsewhere
- **Color**: Color of the object icon as it appears in SmartConsole
- **Network Security**: Select Software Blades on this VSX Cluster and its Cluster Members

VSX Cluster Members

The **Cluster Members** page lets you view and modify several properties for individual VSX Cluster Members, including IP addresses for Cluster Members and the Internal Communication Network.

Gateway VSX Cluster Member List

The **Cluster Members** page shows all the VSX Cluster Members.

To edit a VSX Cluster Member:

From the **Cluster Member** page, select a VSX Cluster Member and click **Edit**.

The **Cluster Member Properties** window opens. These are the settings that you can edit:

- **General** tab:
  - **Comment**: Free text comment that appears in the Object List and elsewhere
  - **Color**: Color of the object icon as it appears in SmartConsole
  - **Secure Internal Communication**: Check and reset SIC trust
- **Topology** tab: Displays the Cluster Member IP address and Net Mask for each interface. Double-click an interface to see its properties.
- **NAT** tab: Define NAT rules for VSX Cluster Members connected to a Virtual Router.
- **VPN** tab: Contains a variety of configuration properties for Site-To-Site VPN deployments.

  This window is only available if the **IPsec VPN** is enabled on the **General Properties** page.

For more about VPN concepts and configurations, see the *R82 Site to Site VPN Administration Guide*.

Where Used

Click **Where used** to show information about the selected member in the objects database.

- **Name**: Cluster name.
- **Table**: Name of the table in the database under which the selected object is listed.
- **Is removable**: Specifies whether or not you are allowed to remove the selected object. If the object is not removable and nevertheless you choose to remove it, it will impact the database or Rule Base.
- **Refresh**: Click to update the window display if you make changes.
- **Context**: Where the object is used.

Internal IP Address and Net Mask

VSX creates an internal communication network and automatically assigns it an IP address and net mask from a predefined pool. You can change this IP address here if you have not yet defined a Virtual System. Although traffic from this address is never sent to any networks, you must ensure that this IP address is unique and not in use anywhere on your defined network.

ClusterXL

To manage state synchronization, open the **ClusterXL** window, or run the *"vsx_util" on page 322* command on the Management Server.

- Enable or disable state synchronization.
- Select tracking options for VSX Cluster Member state changes.

All other ClusterXL configuration properties are disabled.

Physical Interfaces

The **Physical Interfaces** page allows you to add or delete a physical interface on the VSX Gateway, and to define interfaces to be used as VLAN trunks.

- To add a new physical interface, click **Add** and enter the interface name in the appropriate field.
- To define an interface as a VLAN trunk, select the applicable interface and enable the VLAN Trunk option. To disable a VLAN trunk, clear the option.

Synchronization

The **Synchronization** window displays the state synchronization network. There are no configurable properties.

Topology

On the **Topology** page, you can see and configure interface and routing definitions.

Interfaces

The Interfaces section defines interfaces and links to devices. You can add new interfaces as well as delete and modify existing interfaces.

To add an interface:

1. Click **New** and select one of these options:
   - **Regular** - Create a new interface
   - **State Synchronization**
   - **Leads to Virtual Router**
   - **Leads to Virtual Switch**

   The **Interface Properties** window opens.

   Click **Actions** > **Copy to Clipboard** to copy the **Interfaces** table in CSV format.
2. Define the appropriate properties.
3. Click **OK**.

To change an interface:

1. Double-click an interface.

   The **Interface Properties** window opens.
2. Change the parameters for the interface.
3. Click **OK**.

To delete an interface:

1. From the **Topology** page, select the interface and click **Delete**.
2. Click **OK**.

Routes

The **Routes** section of the **Topology** window defines routes between network devices, network addresses, and Virtual Devices. Some routes are defined automatically based on the interface definitions. You can add, change, and delete routes.

To add a default route to the routing table:

1. Click **Add Default Route**.

   The **Default Gateway** window opens.
2. Enter the default route IP address or select the default Virtual Router.
3. Click **OK**.

   The default route is added to the routing table.
4. Select the default route and click **Edit**.

   The **Route Configuration** window opens.
5. Configure the settings for the default route.
6. Click **OK**.

To add a new route to the routing table:

1. Click **Add**.

   The **Route Configuration** window opens.
2. Configure the **Destination** IP address and netmask.
3. Configure the next hop IP address or Virtual Router.
4. **Optional:** Select **Propagate route to adjacent Virtual Devices** to "advertise" the route to neighboring Virtual Devices, and enable connectivity between them.
5. Click **OK**.

To change a route:

1. Select the route.
2. Click **Edit**.

   The **Route Configuration** window opens.
3. Change the settings.
4. Click **OK**.

To delete a route:

1. Select the route.
2. Click **Remove**.

   A confirmation window opens.
3. Click **OK**.

Calculating Topology Automatically Based on Routing Information

Enable this option to allow VSX to automatically calculate the network topology based on interface and routing definitions (enabled by default). VSX creates automatic links, or connectivity cloud objects linked to existing internal or external networks.

- This option is not available in Bridge mode.
- When employing dynamic routing, it is recommended to disable this option.

VPN Domain

The **VPN Domain** section in the **Topology** page defines the set of hosts that use a VPN tunnel to communicate with peer Virtual Systems.

Define a VPN Domain to include a Virtual Device as part of the VPN connection. The domain defines the Virtual System interfaces that are in the VPN. You can define a VPN Domain in different ways:

- **All IP Addresses behind Cluster Members are based on topology information**: Includes all hosts not located behind an external VSX Cluster Member interface.
- **Manually Defined**: Includes all hosts in the selected network or group.
- **Remote Access Communities**: Define an alternative VPN domain for Remote Access Community traffic.

To specify the VPN domain:

1. Click **Set domain for Remote Access Community**.

   The **VPN Domain per Remote Access Community** window opens.
2. Double-click a Remote Access Community.

   The **Set VPN Domain** window opens.
3. Select a VPN domain from the list, or click **New**, to define a new domain.
4. Click **OK**.

NAT

The **NAT** > **Advanced** page lets you configure NAT rules for packets originating from a Virtual System.

To enable and configure NAT for a Virtual System:

1. Select **Add Automatic Address Translation**.
2. Select a translation method:
   - **Hide**: Hide NAT only allows connections originating from the internal network. Internal hosts can access internal destinations, the Internet and other external networks. External sources cannot initiate a connection to internal network addresses.
   - **Static**: Static NAT translates each private address to a corresponding public address.
3. If you select **Hide**, select one of these options:
   - **Hide behind Gateway** hides the real IP address behind the Virtual System external interface IP address,

     or
   - **Hide behind IP Address** hides the real address behind a virtual IP address, which is a routable, public IP address that does not belongs to any real machine.
4. If you selected **Static NAT**, enter the static IP address in the appropriate field.
5. Select the VSX Gateway from the **Install on Gateway** list.

VSX Bridge Configuration

The **VSX Bridge Configuration** page allows you to specify the loop detection algorithm when working in the Bridge mode.

Enable the **Check Point ClusterXL** option to enable the **Active/Standby Bridge Mode** loop detection algorithms contained in ClusterXL.

Enable the **Standard Layer 2 Loop Detection Protocols** to use standard loop detection protocols, such as STP or PVST+.

See *"Bridge Mode" on page 270*.

Changing the Cluster Management IP and/or Subnet

To add, change or delete the cluster management IP address and/or subnet, run the *"vsx_util change_mgmt_ip" on page 333* and *"vsx_util change_mgmt_subnet" on page 334* commands on the Management Server.

Changing the Internal Communication Network IP

You can change the internal communication network IP address by using the *"vsx_util change_private_net" on page 336* command on the Management Server.

Working with VSX Cluster Members

Important - This section does not apply to Scalable Platforms (Maestro and Chassis).

This section presents procedures for adding and deleting VSX Cluster Members.

Adding a New VSX Cluster Member

Important - Make sure that no other administrators are connected to the Management Server before you perform this procedure.
The "`vsx_util`" command cannot modify the management database, if the database is locked because other administrators are connected.

1. Install the new VSX Cluster Member.

   See the *R82 Installation and Upgrade Guide*.

2. Close all SmartConsole windows.
3. Create a full backup of the environment (see sk100395).
4. Connect to the command line on the Management Server.
5. Log in the Expert mode.
6. Run this command and follow the on-screen instructions:

   ```
   vsx_util add_member
   ```

   a. Enter the IP address of the Security Management Server or Main Domain Management Server.

   b. Enter the Management Server administrator user name and password.

   c. Follow the on-screen instructions.

7. Wait until the **"add member operation finished successfully"** message appears, indicating that the database has been successfully updated and saved.

   Note - In a Multi-Domain Server environment, this operation skips all Domain Management Servers locked by an administrator.
   If this should occur, run the command again for the affected Domain Management Servers after they become available.

8. This prompt appears:

   ```
   Do you wish to reconfigure the new VSX gateway/VSX cluster
   member
   ```

- To reconfigure now (recommended), enter "y" and then:
  a. Wait until the "**Reconfigure module operation completed successfully**" summary notice appears.
  b. Reboot the new VSX Cluster Member.
- To reconfigure later, enter "n" and later follow these mandatory steps:
  a. Close all SmartConsole windows.
  b. Connect to the command line on the Management Server.
  c. Log in the Expert mode.
  d. Run this command and follow the on-screen instruction:

     ```
     vsx_util reconfigure
     ```

  e. Wait until the **Reconfigure module operation completed successfully** summary notice appears.

     Note - In a Multi-Domain Server environment, this operation skips all Domain Management Servers locked by an administrator.
     If this should occur, run the command again for the affected Domain Management Servers after they become available.

  f. Reboot the new VSX Cluster Member.

9. Connect to the command line on each VSX Cluster Member.
10. Examine the VSX Cluster configuration:

    ```
    cphaprob state
    ```

11. If the VSX Cluster runs in the VSLS mode:
    a. Connect to the command line on the Management Server.
    b. Log in the Expert mode.
    c. Redistribute Virtual Systems to the newly added VSX Cluster Member:

       ```
       vsx_util vsls
       ```

    d. Connect to the command line on each VSX Cluster Member.
    e. Examine the VSX Cluster configuration:

       ```
       cphaprob state
       ```

Deleting a VSX Cluster Member

Important - Make sure that no other administrators are connected to the Management Server before you perform this procedure. The `vsx_util` command cannot modify the management database if the database is locked.

1. Close all SmartConsole windows.
2. Create a full backup of the environment (see sk100395).
3. Detach the license from the VSX Cluster Member to be removed.

   Otherwise, you cannot remove a VSX Cluster Member.
4. Close all SmartConsole windows.
5. Connect to the command line on the Management Server.
6. Log in the Expert mode.
7. Run this command and follow the on-screen instructions:

   ```
   vsx_util remove_member
   ```

   a. Enter the IP address of the Security Management Server or Main Domain Management Server.

   b. Enter the Management Server administrator user name and password.

   c. Enter "`y`" to confirm that you have detached the license from the VSX Cluster Member.

   d. Select the VSX Cluster.

   e. Select the VSX Cluster Member.

   f. Enter "`y`" to confirm that the VSX Cluster Member to be removed is disconnected.
8. Wait until the **remove member operation finished successfully** message appears.

   Note - In a Multi-Domain Server environment, this operation skips all Domain Management Servers locked by an administrator.
   If this should occur, run the command again for the affected Domain Management Servers after they become available.

   The management database is now updated and saved.
9. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages the VSX Cluster.
10. From the left navigation panel, click **Gateways & Servers**.
11. Double-click the VSX Cluster object.

12. From the left tree, click **Cluster Members**.
13. Make sure you do not see an object representing the removed VSX Cluster Member.

Changing the VSX Cluster Type

Important - This section does not apply to Scalable Platforms (Maestro and Chassis).

Important:

- The only mode available for a VSX Cluster that was installed as R81.10 and higher is **Virtual System Load Sharing (VSLS)**.
- The **High Availability** mode is available only if you upgrade a VSX Cluster from R81 or lower to R82.
  You can also convert a VSLS cluster to the High Availability mode.

This section presents procedures for converting VSX Cluster between High Availability and VSLS.

Changing the VSX Cluster mode involves the use of the "`vsx_util convert_cluster`" command on the Management Server.

Converting from VSLS to High Availability

1. **Redistribute all Active Virtual Systems to one VSX Cluster Member**

   a. Close all SmartConsole windows.

   b. Connect to the command line on the Management Server.

   c. Log in to the Expert mode.

   d. Run:

   ```
   vsx_util vsls
   ```

   e. Enter the IP address for the Security Management Server or Domain Management Server that manages this VSX Cluster.

   f. Enter the Management Server administrator user name and password.

   g. Select the VSX Cluster.

   h. From the Load Sharing menu, enter **3. Set all VSs active on one member**.

   i. Enter the number of the VSX Cluster Member that is hosting the Active Virtual Systems.

   j. Enter **Y** to save and apply the configuration.

   k. Exit the VSLS menu.

2. **Disable the VSLS options**

Perform these steps on each VSX Cluster Member:

a. Connect to the command line.

b. Log in to the Expert mode.

c. Run:

```
cpconfig
```

d. Disable the **Per Virtual System State**.

e. Disable the **ClusterXLfor Bridge Active/Standby**.

f. Restart the Check Point services (this can cause cluster failover):

```
cpstop ; cpstart
```

3. **Convert the VSX Cluster to High Availability**

a. Connect to the command line on the Management Server.

b. Log in to the Expert mode.

c. Run:

```
vsx_util convert_cluster
```

See *"vsx_util convert_cluster" on page 338*.

Important - It is not supported to run the `vsx_util convert_cluster` command to convert a VSX Cluster from the High Availability mode to the VSLS mode when the VSX Cluster contains a Virtual Switch that is not assigned to any physical interface or to a VLAN interface.

d. Enter the IP address for the Security Management Server or Main Domain Management Server that manages this VSX Cluster.

e. Enter the Management Server administrator user name and password.

f. From the Load Sharing menu, enter **3. Set all VSs active on one member**.

g. Select the VSX Cluster.

h. Enter:

```
HA
```

i. Reboot each VSX Cluster Members (this can cause cluster failover).

j. On each VSX Cluster Member:

   i. Connect to the command line.

   ii. Log in to the Expert mode.

   iii. Examine the VSX configuration:

   ```
   vsx stat -v
   ```

   iv. Examine the VSX Cluster state and configuration:

   ```
   cphaprob state
   ```

When the "`vsx_util convert_cluster`" command finishes, there should be only one Active VSX Cluster Member, on which all Virtual Systems are in the **Active** state, and one Standby VSX Cluster Member, on which all Virtual Systems are in the **Standby** state. Any additional VSX Cluster Members should be in **Standby** state, and their Virtual Systems in the **Down** state.

Converting from High Availability to VSLS

Note - You cannot convert a VSX Cluster to the VSLS mode, if it contains Virtual Systems in the Active/Active Bridge Mode, or contains Virtual Routers.

Procedure

1. Close all SmartConsole windows.
2. On each VSX Cluster Member:
   a. Connect to the command line.
   b. Log in to the Expert mode.
   c. Run:

   ```
   cpconfig
   ```

   d. Enable the **Per Virtual System State**.
   e. Enable **ClusterXL for Bridge Active/Standby**.
   a. Restart the Check Point services:

   ```
   cpstop ; cpstart
   ```

3. On the Management Server:
   a. Connect to the command line.
   b. Log in to the Expert mode.
   c. Run:

   ```
   vsx_util convert_cluster
   ```

   See *"vsx_util convert_cluster" on page 338*.

   d. Enter the IP address of the Security Management Server or Domain Management Server that manages this VSX Cluster.
   e. Enter the Management Server administrator user name and password.
   f. Select the VSX Cluster.
   g. Enter:

   ```
   LS
   ```

h. In the prompt "`Proceed with conversion?`", enter:

```
y
```

i. Select an option to distribute Virtual Systems among VSX Cluster Members:

- Distribute all Virtual Systems equally.
- Set all Virtual Systems as **Active** on the same VSX Cluster Member.

4. Reboot each VSX Cluster Member.
5. On each VSX Cluster Member:
   a. Connect to the command line.
   b. Log in to the Expert mode.
   c. Examine the VSX configuration:

```
vsx stat -v
```

   d. Examine the VSX Cluster state and configuration:

```
cphaprob state
```

Configuring Virtual System Load Sharing (VSLS)

In This Section:

Introduction 213
Requirements 216
Virtual System Priority 216
Virtual System Weight 217
Virtual System States 217
Normalized VSLS Deployment Scenario 218
VSX Cluster Member Failure Scenario 219
Virtual System Failure Scenario 221
Failure Recovery 222
Configuring a VSX Cluster in VSLS Mode 223
Viewing VSLS Status 226
Distributing Virtual Systems Between VSX Cluster Members 227
Exporting and Importing VSLS Configuration 229
Virtual Routers in VSLS Mode 232

Important - This section does not apply to Scalable Platforms (Maestro and Chassis). On Scalable Platforms, use the Gaia gClish command "`set cluster configuration high-availability mode 3`".
See the:

- *Maestro Administration Guide* for your version > Chapter "Dual Site in Active/Standby High Availability Mode".
- *Scalable Chassis Administration Guide* for your version > Chapter "Dual Chassis in Active/Standby High Availability Mode".

Introduction

VSX Clusters can efficiently balance network traffic load by distributing active Virtual Systems between VSX Cluster Members.

This capability is known as **Virtual System Load Sharing (VSLS)**.

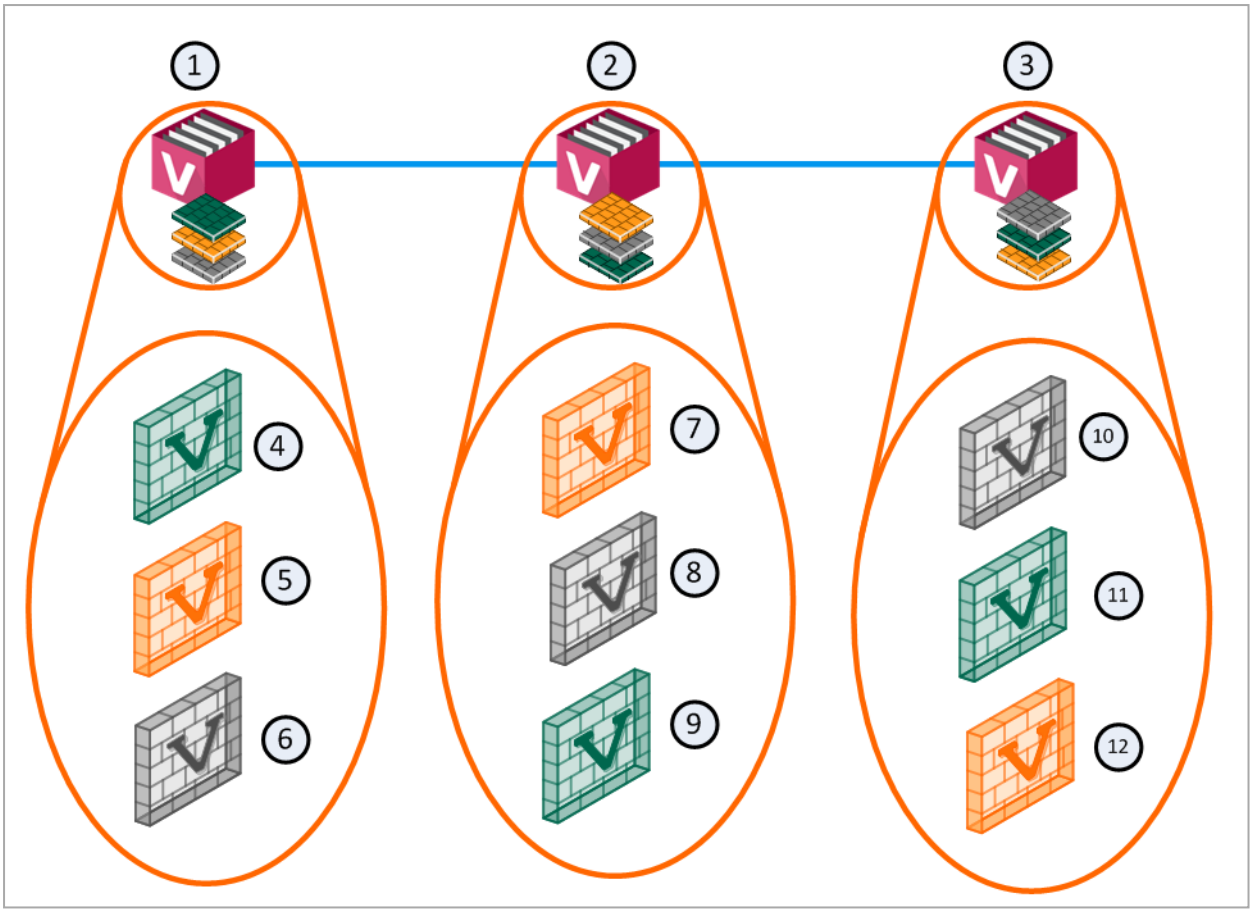
Virtual System Load Sharing is a cluster technology that assigns traffic for Virtual Systems to different Active VSX Cluster Members, which has these benefits:

- **Capacity**: VSLS leverages the cluster machines to handle greater network volume by efficiently dividing the load.
- **Redundancy**: VSLS gives full redundancy by maintaining connectivity for all Virtual Systems even when individual VSX Cluster Members fail.
- **Scalability:** VSLS provides linear scalability for throughput and session rate.
- **Cost Effectiveness**: A VSLS cluster uses standard network switches to get cost effective Load Sharing.
- **Ease of Configuration**: Virtual Systems are automatically distributed between all the VSX Cluster Members - no special configuration is required.
- **Priority Designation**: Mission-critical Virtual Systems can be separated from the other Virtual Systems to utilize better bandwidth and resources.
- **System Scalability**: Every VSX Cluster Member added to the cluster increases the overall system capacity and redundancy.

Important - These Virtual Devices are not supported when the Per-Virtual System state is enabled:

- Virtual Routers
- Virtual Switches without physical or VLAN interfaces

In an example deployment scenario with three VSX Cluster Members, each with three Virtual Systems: an equalized Load Sharing deployment might have one Active Virtual System on each VSX Cluster Member.



Item	Description		Item	Description
1	VSX Cluster Member 1		8	Virtual System 2 is Backup
2	VSX Cluster Member 2		9	Virtual System 3 is Active
3	VSX Cluster Member 3		10	Virtual System 1 is Backup
4	Virtual System 1 is Active		11	Virtual System 2 is Active
5	Virtual System 2 is Standby		12	Virtual System 3 is Standby
6	Virtual System 3 is Backup		———	Sync Network
7	Virtual System 1 is Standby			

A different member hosts the active peer for each Virtual System. This distribution spreads the load equally between the VSX Cluster Members.

When you create a Virtual System, VSX automatically assigns Standby and Backup states to the applicable peers and distributes them between the other VSX Cluster Members.

In the event that a VSX Cluster Member fails, VSLS directs traffic destined to affected Virtual Systems to their fully synchronized Standby peers, which then become Active. At the same time, a Backup Virtual System switches to Standby, and synchronizes with the newly Active Virtual System.

In the event that an individual active Virtual System fails, it immediately fails over to its Standby peer and one of its Backup peers becomes the Standby, synchronizing with the newly Active peer.

VSLS lets administrators manually assign Virtual Systems to specified VSX Cluster Members, or lets VSX automatically assign Virtual System traffic dynamically.

Requirements

All Virtual Systems in all VSX Cluster Members must have direct connectivity with each other.

Connectivity must be accomplished using switches or VLAN connections.

This is required for detecting and assigning Virtual System states.

Virtual System Priority

Virtual System priority refers to a preference regarding which VSX Cluster Member hosts a Virtual System's Active, Standby, and Backup states.

This preference is expressed as an integer value.

Priority	Definition
0	Highest priority, indicating the cluster designated to host the Virtual System **Active** state.
1	Second highest priority, indicating the member designated to host the Virtual System **Standby** state.
> 1	Lower priorities, indicating the VSX Cluster Members designated to host a Virtual System **Backup** state. The VSX Cluster Member assigned priority 2 is the first to switch the Virtual System to the Standby state in the event of a failure of either the Active or Standby Virtual System. A VSX Cluster Member assigned priority 3 is the next in line to come online in the event of another failure.

You can change the priority designation with the "`vsx_util vsls`" command on the Management Server.

Virtual System Weight

Because not all Virtual Systems are equal in terms of traffic and load, VSLS allows you to assign "weights" to individual Virtual Systems.

The weight of a Virtual System affects the dispersal pattern of other Virtual Systems across VSX Cluster Members.

When you assign a heavier weight to a Virtual System gives it a larger share of resources on a specific VSX Cluster Member, and disperses the other Virtual Systems to other VSX Cluster Members.

By default, all Virtual Systems are assigned an equal weight factor of 10.

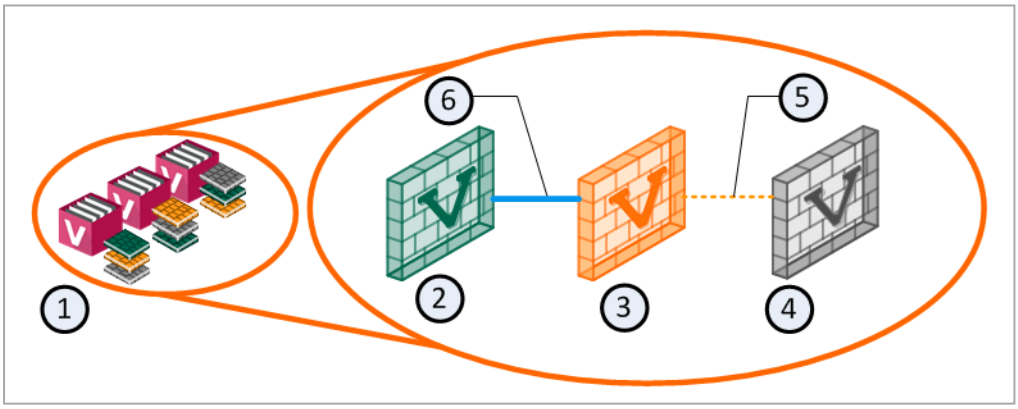
You can change the weight factor with the "`vsx_util vsls`" command on the Management Server.

Virtual System States

VSLS adds a Backup state to the existing Active and Standby states.

The Backup state contains the latest configuration settings for each Virtual System, but does not receive state table synchronization.

The figure below illustrates the relationship between Virtual System states.



Item	Description
1	VSX Cluster with 3 Cluster Members, each running 3 Virtual Systems (2, 3, and 4)
2	Virtual System 1 on VSX Cluster Member 1 is Active
3	Virtual System 1 on VSX Cluster Member 2 is Standby
4	Virtual System 1 on VSX Cluster Member 3 is Backup
5	Policy updates only
6	State tables are synchronized

Each Virtual System peer in a VSLS cluster is replicated on all VSX Cluster Members, and each copy exists in a different state.

The Active and Standby states are synchronized, so that the Standby peer can immediately become Active in the event of a failure of the Active Virtual System or VSX Cluster Member.

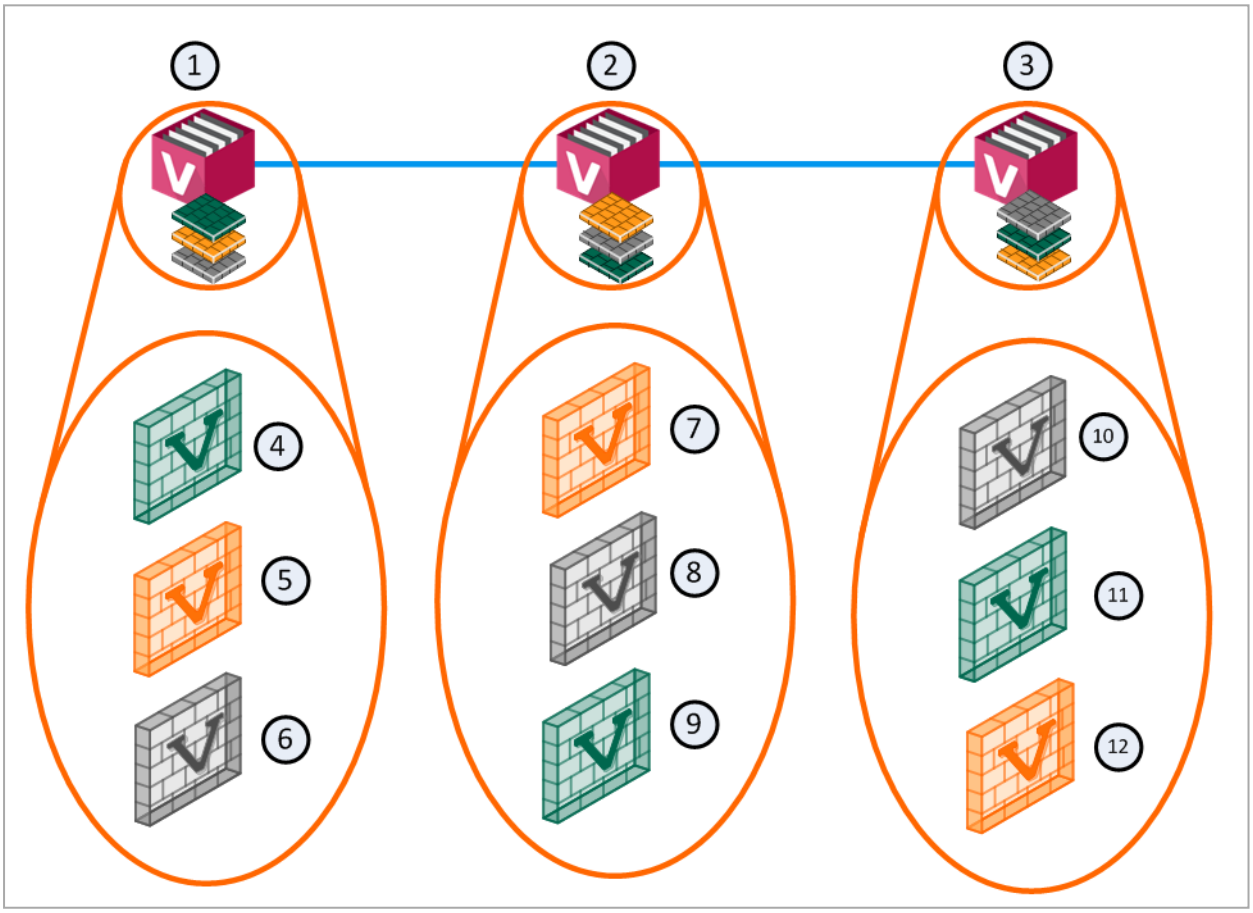
When this happens, the Backup peer becomes the Standby, and immediately synchronizes with the new Active Virtual System.

VSLS reduces the load on the synchronization network by not synchronizing the Backup Virtual System state tables with the Active Virtual System until a failover occurs.

Normalized VSLS Deployment Scenario

For example, you can have three VSX Cluster Members, each with three Virtual Systems.

In this configuration, an equalized Load Sharing deployment could have one Active Virtual System on each VSX Cluster Member.



Item	Description		Item	Description
1	VSX Cluster Member 1		8	Virtual System 2 is Backup
2	VSX Cluster Member 2		9	Virtual System 3 is Active

Item	Description		Item	Description
3	VSX Cluster Member 3		10	Virtual System 1 is Backup
4	Virtual System 1 is Active		11	Virtual System 2 is Active
5	Virtual System 2 is Standby		12	Virtual System 3 is Standby
6	Virtual System 3 is Backup		———	Sync Network
7	Virtual System 1 is Standby			

A different VSX Cluster Member can host the Active state of each Virtual System.

This distribution of Virtual Systems spreads the load between the VSX Cluster Members.

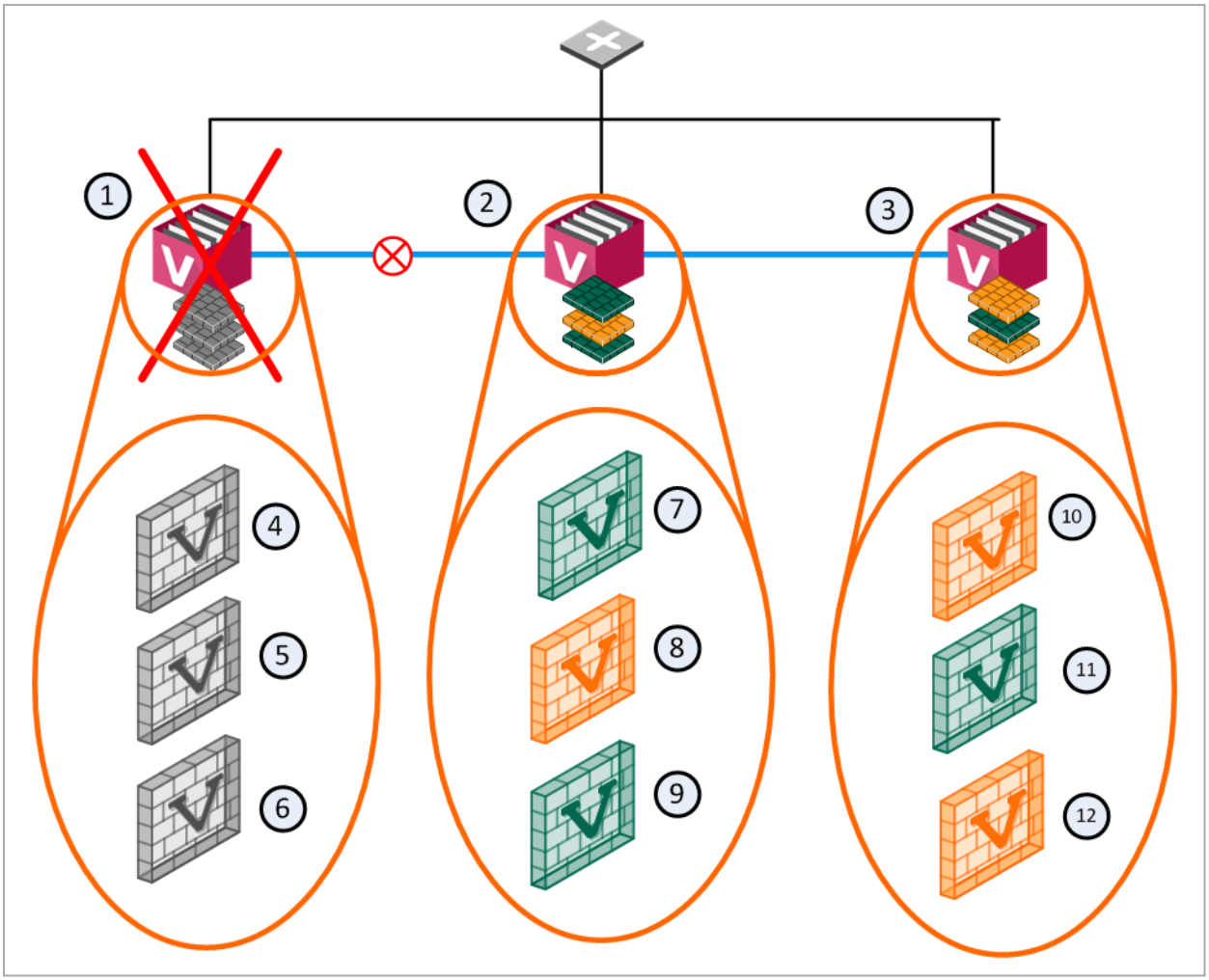
When a Virtual System is created, the system automatically creates Standby and Backup states and distributes them between the other VSX Cluster Members.

VSX Cluster Member Failure Scenario

In the event that a member fails or experiences a connectivity problem, VSLS detects the problem and routes traffic for the affected Virtual Systems to their corresponding Standby Virtual Systems.

Standby Virtual Systems, which are fully synchronized with their active peers, change immediately to the Active state and preserve active connections.

At the same time, the backup Virtual Systems switch to Standby, and synchronize fully with the newly active Virtual Systems.



Item	Description		Item	Description
1	VSX Cluster Member 1		8	Virtual System 2 is Standby
2	VSX Cluster Member 2		9	Virtual System 3 is Active
3	VSX Cluster Member 3		10	Virtual System 1 is Standby
4	Virtual System 1 is Down		11	Virtual System 2 is Active
5	Virtual System 2 is Down		12	Virtual System 3 is Standby
6	Virtual System 3 is Down			Sync Network
7	Virtual System 1 is Active			Network Traffic

In this scenario, VSX Cluster Member 1 fails and its Active and Standby Virtual Systems fail over to VSX Cluster Member 2 and VSX Cluster Member 3.

The Active Virtual System (VS1) moves to VSX Cluster Member 2 and directs all VS1 traffic itself.

Its Backup peer on VSX Cluster Member 3 synchronizes with the new Active Virtual System and becomes the Standby.

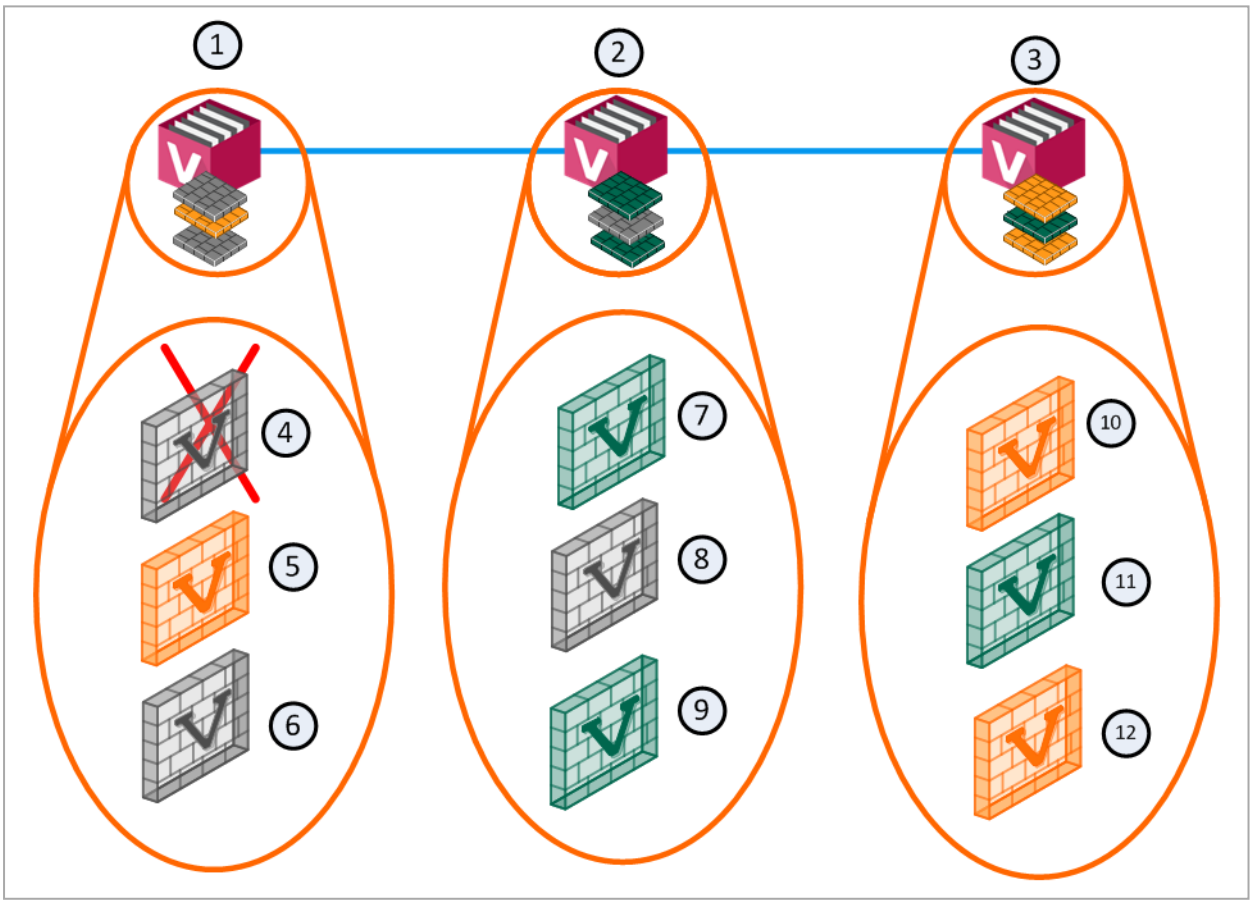
VS2 on VSX Cluster Member 2 becomes the Standby and synchronizes with the Active peer on VSX Cluster Member 3.

For VS3, the Active and Standby peers remain the same.

Virtual System Failure Scenario

In a failure scenario where an active Virtual System fails on one member, but the Standby and Backup Virtual Systems remain up: the Active Virtual System fails over to its Standby peer, and its Backup becomes the Standby.

The new Standby synchronizes with the new Active member.



Item	Description		Item	Description
1	Member 1		8	VS 2 Backup

Item	Description		Item	Description
2	Member 2		9	VS 3 Active
3	Member 3		10	VS 1 Standby
4	VS 1 Down		11	VS 2 Active
5	VS 2 Standby		12	VS 3 Standby
6	VS 3 Backup		——	Sync Network
7	VS 1 Active			

All other Virtual Systems continue to function as usual, and no failover occurs.

Failure Recovery

When the failed VSX Cluster Member or Virtual System comes back online, the system returns to its original Load Sharing configuration.

Configuring a VSX Cluster in VSLS Mode

1. **Install the VSX Cluster Members**

   See the *R82 Installation and Upgrade Guide* - Chapter *Installing a ClusterXL, VSX Cluster, VRRP Cluster* - Section *Installing a VSX Cluster*.

2. **Enable the Per Virtual System State mode on each VSX Cluster Member**

   The **Per Virtual System State** mode enables active Virtual Systems to be placed on different VSX Cluster Members, and for Virtual System-specific failover. This setting is mandatory for VSLS.

   On each VSX Cluster Member:

   a. Connect to the command line.

   b. Log in to the Expert mode.

   c. Run:

   ```
   cpconfig
   ```

   d. Select:

   Enable Check Point Per Virtual System State

   e. When the question appears:

   ```
   Would you like to enable Per Virtual System state?
   ```

   Enter **y** to confirm.

   f. Reboot the VSX Cluster Member.

3. **In SmartConsole, create a new VSLS VSX Cluster object**

   a. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages the VSX Cluster.

   b. From the navigation panel, click **Gateways & Servers**.

   c. At the top, click **Objects** menu **> More object types > Network Object > Gateways and Servers > VSX > New Cluster**.

   The **VSX Cluster Wizard** > **General Properties** opens.

d. Create and configure the new VSX Cluster.

   See *"Working with VSX Clusters" on page 191*.

   i. On the **General Properties** page, from **VSX Cluster Platform,** select **ClusterXL Virtual System Load Sharing**.

   ii. Complete the VSX Cluster Wizard.

4. **In SmartConsole, create the objects of applicable Virtual Routers and Virtual Systems**

   See:

   - *"Working with Virtual Routers" on page 132*
   - *"Working with Virtual Systems" on page 109*

5. **Use the '`vsx_util vsls`' command on the Management Server**

   Use the "`vsx_util vsls`" command (see *"vsx_util vsls" on page 357*) on the Management Server to do different Virtual System Load Sharing configuration tasks:

   - Show the current VSLS configuration
   - Distribute Virtual Systems equally between VSX Cluster Members
   - Set all Virtual Systems as Active on one VSX Cluster Member
   - Manually define the priority and weight for individual Virtual Systems
   - Toggle VSLS mode between Active Up and Primary Up
   - Import VSLS configuration from CSV text files
   - Export VSLS configuration to CSV text files

   Procedure:

   a. Connect to the command line on the Management Server.

   b. Log in to the Expert mode.

   c. Run:

   ```
   vsx_util vsls
   ```

   d. Enter the IP address of the Security Management Server or Domain Management Server.

   e. Enter the Management Server administrator user name and password.

f. Select the applicable option from the VSLS menu.

Example

```
[Expert@MGMT:0]# vsx_util vsls
Enter Security Management Server/main Domain Management Server IP address (Hit
'ENTER' for 'localhost'): 172.16.16.240
Enter Administrator Name: admin
Enter Administrator Password: ****

Select VSX gateway/cluster object name:
1)    VSX_Cluster_1
2)    VSX_Cluster_2
3)    VSX_GW_1
4)    VSX_GW_2
Select: 1


VS Load Sharing - Menu
__________________________________
1. Display current VS Load sharing configuration
2. Distribute all Virtual Systems so that each cluster member is equally loaded
3. Set all VSes active on one member
4. Manually set priority and weight
5. Toggle VSLS mode between Active Up and Primary Up
6. Import configuration from a file
7. Export configuration to a file
8. Exit

Enter redistribution option (1-8) [1]:
```

Viewing VSLS Status

To view the current VSLS status and Virtual System distribution between VSX Cluster Members, select **Display current VS Load Sharing configuration** from the VSLS menu.

Example

```
----+---------+-----------+-----------+-----------+--------+
VSID| VS name | gw150     | gw151     | gw152     | Weight |
----+---------+-----------+-----------+-----------+--------+
 2  | vs1     | 0         | 1         | 2         | 10     |
 3  | vs2     | 2         | 0         | 1         | 10     |
 4  | vs3     | 1         | 2         | 0         | 10     |
 5  | vs5     | 0         | 2         | 1         | 10     |
  6 | vs4     | 1         | 0         | 2         | 10     |
----+---------+-----------+-----------+-----------+--------+
 Total weight | 20        | 20        | 10        | 50     |
----+---------+-----------+-----------+-----------+--------+

Legend:
0 - Highest priority
1 - Next priority
2 - Lowest priority
```

Virtual System Priority

Virtual System priority refers to a preference regarding which VSX Cluster Member hosts a Virtual System's Active, Standby, and Backup states.

This preference is expressed as an integer value.

Priority	Definition
0	Highest priority, indicating the VSX Cluster Member designated to host the Virtual System**Active** state.
1	Second highest priority, indicating the VSX Cluster Member designated to host the Virtual System**Standby** state.
> 1	Lower priorities, indicating VSX Cluster Members designated to host a Virtual System's **Backup** state. The VSX Cluster Member assigned priority 2 will be the first to switch the Virtual System to the Standby state in the event of a failure of either the Active or Standby Virtual System. A VSX Cluster Member assigned priority 3 would be the next in line to come online in the event of another failure.

Virtual System Weight

Each Virtual System is assigned a weight factor, which determine its traffic volume relative to the total traffic volume (the sum of all weight factors) on a given VSX Cluster Member.

VSX uses the weight factor to determine the most efficient distribution of Virtual Systems between VSX Cluster Members.

System resource allocation is not affected by the weight factor, and VSX does not take weight into consideration for any other purpose.

By default, all Virtual Systems are assigned an equal weight factor of 10.

Distributing Virtual Systems Between VSX Cluster Members

The primary advantage of VSLS is that it distributes Active, Standby and Backup Virtual Systems between VSX Cluster Members to maximize throughput and user response time.

You can distribute Virtual Systems in one of these ways:

Automatically distribute Active Virtual Systems between VSX Cluster Members

This lets you automatically distribute Active Virtual Systems between VSX Cluster Members, so that all VSX Cluster Members are equally loaded, based on assigned weights and existing or default priority definitions.

1. From the VSLS menu (see *"vsx_util vsls" on page 357*), select the VSX Cluster object.
2. Select **Distribute all Virtual Systems so that each cluster member is equally loaded**.
3. At the "`Save & apply configuration?`" prompt, enter **y** to continue.

The update process may take several minutes or longer to complete, depending on the number of Virtual Systems and VSX Cluster Members.

Automatically assign all Active Virtual Systems to the Same VSX Cluster Member

1. From the VSLS menu (see *"vsx_util vsls" on page 357*), select the VSX Cluster object.
2. Select **Set all VSs active on one member**.
3. When prompted, enter the number corresponding to the VSX Cluster Member designated as the Primary member.
4. When prompted, enter the number corresponding to the VSX Cluster Member designated as the Standby member.

   All other VSX Cluster Members are designated as Backup members.
5. At the "`Save & apply configuration?`" prompt, enter **y** to continue.

The update process may take several minutes or longer to complete, depending on the number of Virtual Systems and VSX Cluster Members.

Manually configure priorities and weights for each Virtual System

Note - After you save changes, the update requires time (several minutes or longer), depending on the quantity of Virtual Systems and VSX Cluster Members.

To assign weights automatically to all Virtual Systems

1. From the VSLS menu (see *"vsx_util vsls" on page 357*), select the VSX Cluster object.
2. Select **Manually set priority and weight**.
3. Scroll through each Virtual System. Enter **a**.
4. For each Virtual System, enter a weight value and press **Enter**.

   If you do not enter a weight value for a Virtual System, the assigned weight is not changed.

   Only Virtual Systems with a new weight value are updated.

   To stop entering weight values, enter **s**.
5. At the "`Save & apply configuration`" prompt, enter **y** to continue.

To assign priorities and weights manually to individual Virtual Systems

1. From the VSLS menu (see *"vsx_util vsls" on page 357*), select the VSX Cluster object.
2. Select **Manually set priority and weight**.
3. Enter **m**.
4. At the "`Would you like to change the Virtual System's priority list?`" prompt, enter **y** to continue.
5. Enter the number of the VSX Cluster Member to get the highest priority.
6. Enter the number of the VSX Cluster Member to get the next highest priority.
7. Continue until all VSX Cluster Members have a priority.
8. At the "`Would you like to change the Virtual System's weight?`" prompt, enter **y** to continue.
9. Enter the new weight value. A valid value is an integer between 1 and 100.
10. At the "`Do you wish to configure another Virtual System?`" prompt, enter **y** to configure a different Virtual System, or enter **n** to continue.
11. At the "`Save & apply configuration?`" prompt, enter **y** to continue.

Exporting and Importing VSLS Configuration

When working with large scale VSLS deployments consisting of many Virtual Systems, multiple VSX Cluster Members, using the `vsx_util` command on the Management Server to do configuration tasks can be quite time consuming.

To let administrators to efficiently configure such deployments, VSX supports uploading VSLS configuration files containing configuration information for all Virtual Systems directly to Management Servers and VSX Cluster Members.

This capability offers the following advantages:

- Fast VSLS configuration of large-scale deployments with many Virtual Systems and VSX Cluster Members.
- Efficient migration and scalability for complex deployments.
- External backup of VSLS configurations.

VSLS configuration files are CSV files that are editable using a text editor or other applications, such as Microsoft Excel. You can use the configuration file to change quickly the weight and VSX Cluster Member priority for each Virtual Systems in the list.

Note - You cannot use the VSLS configuration file to add or remove VSX Cluster Members. You must use the applicable `vsx_util` commands to do this.
You can use the VSLS configuration file to change member priorities for Virtual Systems after adding or removing a VSX Cluster Member.

VSLS Configuration File

The VSLS configuration file is a comma separated value (CSV) text file that contains configuration settings for all Virtual Systems controlled by a Management Server.

All lines preceded by the **#** symbol are comments and are not imported into the management database.

Example

```
# Check Point VSX - VS Load Sharing configuration file
#
# Administrator : aa
# SmartCenter/Main Domain Management Server : 192.168.50.160
# Generated on : Thu Jul 23 13:08:42 2009
#
#
#
# VSID, Weight, Active member, Standby member, Backup member #1
# Virtual System name: vs1
2,10,gw150,gw151,gw152

# Virtual System name: vs2
3,10,gw151,gw152,gw150

# Virtual System name: vs3
4,10,gw152,gw150,gw151

# Virtual System name: vs4
6,10,gw151,gw150,gw152

# Virtual System name: vs5
5,10,gw150,gw152,gw151
```

The configuration file contains one line for each Virtual System, consisting of the following data as shown below:

Each line contains the VSID, the weight assigned the Virtual System, one primary VSX Cluster Member, and one Standby VSX Cluster Member.

Backup VSX Cluster Members are listed after the Standby VSX Cluster Member.

Exporting a VSLS configuration

The most common way to use VSLS configuration files is to initially define your cluster environment and Virtual Systems using SmartConsole.

1. From the VSLS menu (see *"vsx_util vsls" on page 357*), select **Export configuration to a file**.
2. Enter the absolute path to the file.

   For example:

   `/home/admin/MyConfiguration.txt`

Processing Options

You can insert the following commands in the VSLS Configuration file to show audit trail information while validating and processing data.

Each of the commands is like a toggle, whereby the first occurrence of a command enables the action and the next occurrence disables it.

These options let you debug efficiently very long configuration files by displaying or logging only suspicious sections of the data.

Command	Action
!comments	Sequentially displays comment lines (those preceded with the '#' character) contained in the configuration file. You can insert comments into the configuration file to indicate which Virtual Systems are currently processed, or to provide status information as the parser processes the data.
!verbose	Shows whether or not each data line has been successfully verified and the configuration parameters for each Virtual System.
!log	Saves `!comments` and `!verbose` information in the `vsx_util.log` file.

Importing a VSLS configuration

1. From the VSLS menu (see *"vsx_util vsls" on page 357*), select **Import configuration from a file**.
2. Enter the absolute path to the file.

   For example:

   `/home/admin/MyConfiguration.txt`
3. At the "`Save & apply configuration?`" prompt, enter **y** to continue.

During the import process, the parser reads the configuration file and attempts to validate the contents.

Errors are displayed on the screen together with the offending line number.

If either the **!comments** or **!verbose** processing options are enabled, the applicable information appears on the screen.

The process update process may take several minutes or longer to complete, depending on the quantity of Virtual Systems, Domain Management Servers, and VSX Cluster Members.

Virtual Routers in VSLS Mode

From R81, you can configure Virtual Routers in VSLS mode.

Description of Virtual Router Groups

To ensure traffic flow during a VSX Cluster failover, a Virtual Router and all Virtual Systems that connect to it belong to the same Virtual Router Group.

The Virtual Router in a Virtual Router Group manages all Virtual Systems in that Virtual Router Group. It makes sure all Virtual Systems are **Active** on the same VSX Cluster Member as the Virtual Router.

If at least one Virtual System or the Virtual Router in the affected Virtual Router Group fail, all Virtual Systems and the Virtual Router in the same Virtual Router Group fail over from the affected VSX Cluster Member to another VSX Cluster Member.

Important:

- A Management Server creates the corresponding Virtual Router Group automatically when you create a Virtual Router object.
- You can connect a Virtual System to only one Virtual Router.
- The cluster state of all members of the same Virtual Router Group is **Active** on the same VSX Cluster Member.
- Changes in the cluster state of Virtual Systems in a Virtual Router Group take effect only after you install the Access Control Policy on the applicable Virtual Systems.
- Connecting an existing Virtual System to an existing Virtual Router:
  If the cluster state of an existing Virtual System is **Active** on *one* VSX Cluster Member, and the cluster state of an existing Virtual Router is **Active** on *another* VSX Cluster Member, then after you connect the Virtual System to this Virtual Router and install the Access Control Policy on the Virtual System, it becomes **Active** on the same VSX Cluster Member as the Virtual Router.

Viewing the existing Virtual Router Groups on a Management Server

Procedure

1. Connect to the command line on the Management Server that manages the VSX Cluster object.
2. Log in to the Expert mode.
3. Go to the configuration menu for Virtual System Load Sharing:

   ```
   vsx_util vsls
   ```

4. From the VSLS menu, select **Display current VS Load sharing configuration**.

In the column "**VS name**":

- After the name of the Virtual Router, in the brackets you see the number of the Virtual Router Group and the letter **M** (denotes the manager of this Virtual Router Group).
- After the name of the Virtual System, in the brackets you see the number of the Virtual Router Group, to which this Virtual System belongs.

Every Virtual Router Group gets a cardinal number:

a. For the first Virtual Router you create, the Management Server creates a Virtual Router Group #1.

b. For the second Virtual Router you create, the Management Server creates a Virtual Router Group #2.

c. And so on.

Example

```
[Expert@MGMT:0]# vsx_util vsls
Enter Security Management Server/main Domain Management Server IP address (Hit
'ENTER' for 'localhost'): 172.16.16.240
Enter Administrator Name: admin
Enter Administrator Password:

Select VSX gateway/cluster object name:
  1)    VSX_Cluster_1
  2)    VSX_Cluster_2
  3)    VSX_GW_1
  4)    VSX_GW_2
Select: 1


VS Load Sharing - Menu
______________________________________
1. Display current VS Load sharing configuration
2. Distribute all Virtual Systems so that each cluster member is equally loaded
3. Set all VSes active on one member
4. Manually set priority and weight
5. Toggle VSLS mode between Active Up and Primary Up
6. Import configuration from a file
7. Export configuration to a file
8. Exit

Enter redistribution option (1-8) [1]: 1

VSLS is in Primary Up mode.

----+----------------+----------+----------+--------+
VSID| VS name        | Member_1 | Member_2 | Weight |
----+----------------+----------+----------+--------+
  1 | VR (1M)        | 0        | 1        | 10     |
  2 | vs1 (1)        | 0        | 1        | 0      |
  3 | vs2            | 1        | 0        | 10     |
  4 | vs3            | 0        | 1        | 10     |
  5 | vs4            | 0        | 1        | 10     |
----+----------------+----------+----------+--------+
 Total weight        | 20       | 20       | 40     |
----+----------------+----------+----------+--------+

Legend:
0 - Highest priority
1 - Lowest priority

Note: Virtual devices that are on the same group are marked with the same number '
(group #)'.
Virtual device that is marked with (<group #> L) is defined as manager of <group #>.
Only a group manager has weight greater than 0, which is the sum of weights of all
group members.
Virtual devices, that are not part of any group, show their own weight.
```

5. Exit from the menu.

Viewing the existing Virtual Router Groups on VSX Cluster Members

Procedure

1. Connect to the command line on the VSX Cluster Member.
2. Log in to the Expert mode.
3. Run:

```
cphaprob show_vsls_groups
```

Notes:

- You can run this command in any VSX context.
- If you run this command in the context of a Virtual Router, you can see the names and VSID of Virtual Systems that belong to the corresponding Virtual Router Group.
  Example - Context of the Virtual Router "VR":

```
[Expert@VSX_Member_1:1]# cphaprob show_vsls_groups
VR vsid 1 is a VSLS group manager.
Group members are:
vs1 vsid 2
vs2 vsid 3
```

- If you run this command in the context of a Virtual System that is connected to a Virtual Router, you can see the VSID of the Virtual Router that manages the corresponding Virtual Router Group.
  Example - Context of the Virtual System "VS1":

```
[Expert@VSX_Member_1:2]# cphaprob show_vsls_groups
vs1 vsid 2 is a VSLS group member.
VSLS Group manager is VR vsid 1
```

VSLS Weights in Virtual Router Groups

When Virtual Systems are connected to a Virtual Router, the weight of the Virtual Router in the corresponding Virtual Router Group is the total sum of all weights of all Virtual Systems.

For Virtual Systems that belong to Virtual Router Groups, outputs of different commands show their weight of as 0 (zero).

For Virtual Systems that do **not** belong to Virtual Router Groups, outputs of different commands show their real weight (by default, all Virtual Systems are assigned an equal weight factor of 10.).

For example, if a Virtual System "vs1" with the wight 20 and a Virtual System "vs2" with the wight 30 are connected to a Virtual Router "vr", then outputs of different commands show the weight of the Virtual Router as 50.

Note - The total sum of all weights of all Virtual Systems in the same Virtual Router Group cannot be more greater than 100.

Distributing Virtual Systems that belong to a Virtual Router Group between VSX Cluster Members

If it is necessary to distribute manually Virtual Systems between VSX Cluster Members, and these Virtual Systems are connected to a Virtual Router, you must distribute the corresponding Virtual Router between VSX Cluster Members (assign the priority and weight only to this Virtual Router). The Management Server automatically distributes all Virtual Systems in the corresponding Virtual Router Group.

For more information, see *"Distributing Virtual Systems Between VSX Cluster Members" on page 227*.

VSX Cluster in the High Availability Mode

Important - This section does not apply to Scalable Platforms (Maestro and Chassis).

Important:

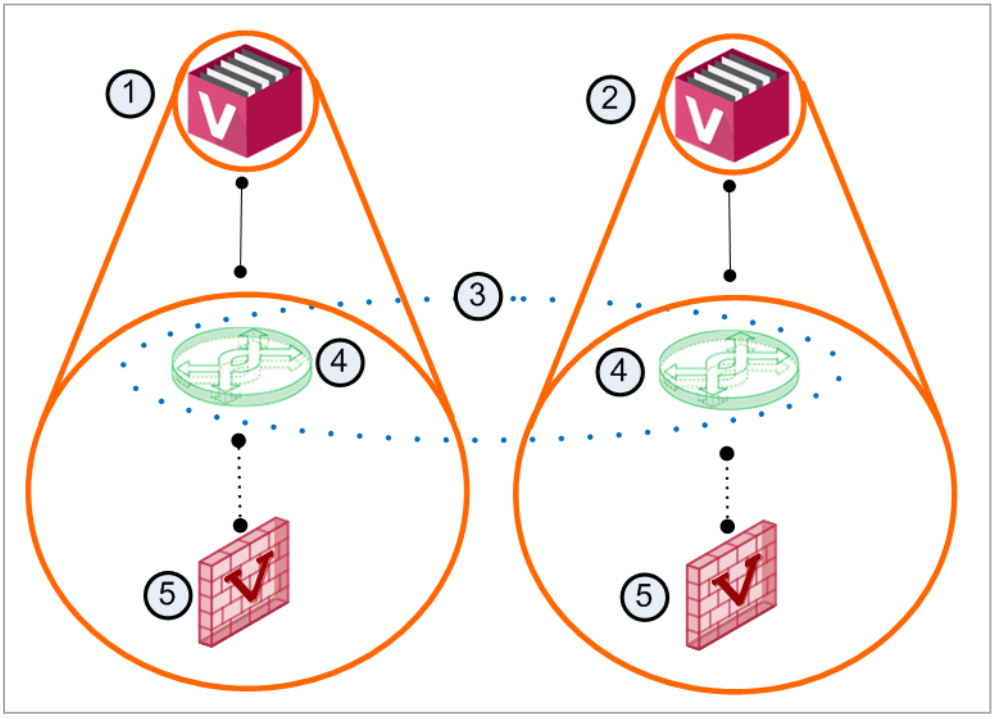
- The only mode available for creating a new VSX Cluster that was installed as R81.10 and higher is **Virtual System Load Sharing (VSLS)**.
- VSX Clusters in the **High Availability** mode that are upgraded from R81 and lower to R81.10 and higher stay in the High Availability mode after the upgrade. You can also convert a VSLS Cluster to the High Availability mode and vice versa (see *"Changing the VSX Cluster Type" on page 208*).

Virtual Switches in a High Availability VSX Cluster

In a VSX Cluster, Virtual Switches are also clustered for redundancy and are defined as *Active/Active.*

The physical interface connected to the Virtual Switch is monitored by means of the Cluster Control Protocol (CCP).

In the event of a failover, all Virtual Systems on the *Standby* VSX Cluster Member become *Active*, and send Gratuitous ARP Requests from the `warp` interface between the Virtual System and the Virtual Switch.



Item	Description
1	Active VSX Cluster Member
2	Standby VSX Cluster Member
3	Virtual Switch Cluster
4	Active Virtual Switch
5	Virtual System 1
	Physical Link
	Warp Link

In the above figure, a simplified VSX Cluster contains two VSX Cluster Members in the High Availability mode, one *Active*, and the other *Standby*.

The Virtual Switches within each VSX Cluster are *Active/Active*.

When the physical interface connected to either Virtual Switch fails to respond, a failover occurs.

Advanced Clustering Configuration

Important - This section does not apply to Scalable Platforms (Maestro and Chassis).

This section presents several advanced cluster scenarios and procedures for their configuration.

Monitoring all VLANs in VSX Cluster

By default, ClusterXL only monitors two VLANS for failure detection and failover.

These are the highest and lowest VLAN tags defined for a given interface.

For example, if the topology for interface eth1 includes several VLAN tags in the range of eth1.10 to eth1.50, ClusterXL only monitors VLANs eth1.10 and eth1.50 for failure. Failures on any of the other VLANs are not detected in the default configuration.

Note - The command "`cphaprob -a if`" (or Gaia Clish command "`show cluster interfaces vlans`") shows the highest and lowest VLANs that are monitored.

When both the highest and lowest VLANs fail, all the VLANs are considered down, and a failover occurs.

This means that if a VLAN, which is **not** listed as the highest or lowest goes down, the VLAN Trunk is still considered "up", and no failover occurs.

There are instances in which it would be advantageous to monitor all the VLANs in the trunk, not just the highest and lowest, and initiate a failover when any one of the VLANs goes down.

To enable monitoring of all VLANs, set the value of the kernel parameter "`fwha_monitor_all_vlan`" to 1 in the `$FWDIR/boot/modules/fwkern.conf` file. For more information, see sk92826 and *"Working with Kernel Parameters" on page 435*.

Configuring CoreXL in a VSLS VSX Cluster

In VSLS VSX Clusters of version R80.10 and higher, changing the CoreXL configuration or running the `cphastop` command in the context of VS0 results in failover of all the Active Virtual Systems on that VSX Cluster Member.

This behavior is by design. Active Virtual Systems on other VSX Cluster Members do not fail over.

Working with Link Aggregation

In This Section:

Link Aggregation Overview 240
How Link Aggregation Works 241
Link Aggregation High Availability 242
Link Aggregation Load Sharing 243
Bond Interface Limitations 243

Link Aggregation Overview

Link aggregation, also known as interface bonding, joins multiple physical interfaces together into a virtual interface, known as a **bond interface**. A bond interface can be configured for High Availability redundancy or for load sharing, which increases connection throughput above that which is possible using one physical interface.

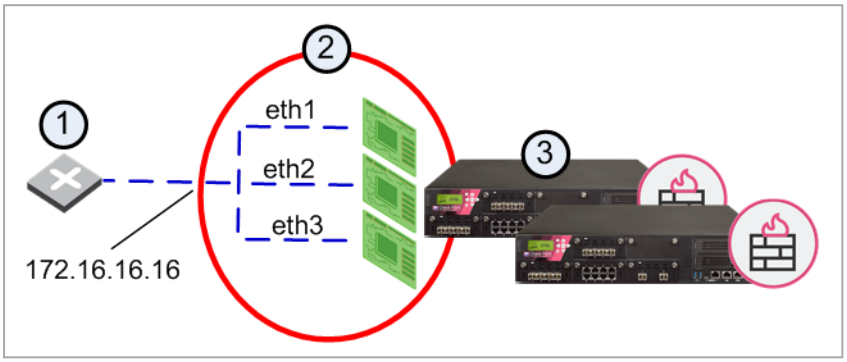
For more about Bond Interfaces (Link Aggregation), see the *R82 Gaia Administration Guide* and *R82 ClusterXL Administration Guide*.

Bonding (Link Aggregation) Terminology

- **Link Aggregation (Interface Bonding)**: Networking technology that binds multiple physical interfaces together into one virtual interface.
- **Bond**: A group of physical interfaces that operate together as one virtual interface and share an IP address and MAC address. A bond is identified by the cluster by its **Bond ID** (for example: `bond0`).
- **Bond Interface**: The logical representation of the bond.
- **Subordinate interface**: A physical interface that is a member of a bond. Subordinate interfaces do not have an IP Address and in some cases share the same MAC address.

How Link Aggregation Works

A bond contains a minimum of one and may contain up to eight subordinate interfaces. All subordinate interfaces contained in a bond share a common IP address and may share the same MAC address. We recommend that each cluster member contain the same quantity of identical subordinate interfaces.



Item	Description
1	Switch
2	bond 0
3	Cluster

You can configure Link Aggregation using one of the following strategies:

- **High Availability (Active/Backup)**: Ensures redundancy in the event of interface or link failure. This option also provides switch redundancy.
- **Load Sharing (Active/Active)**: All interfaces are active, but handle different connections simultaneously. Traffic is balanced amongst subordinate interfaces to maximize throughput. The Load Sharing option does not support switch redundancy.

Link Aggregation High Availability

Clusters, by definition, provide redundancy and high availability at the VSX Gateway level.

Link Aggregation, however, adds interface and switch redundancy by providing automatic failover to a standby interface card within the same VSX Gateway.

In a High Availability deployment, only one interface is active at a time. If an interface or connection fails, the bond fails over to a standby subordinate interface.

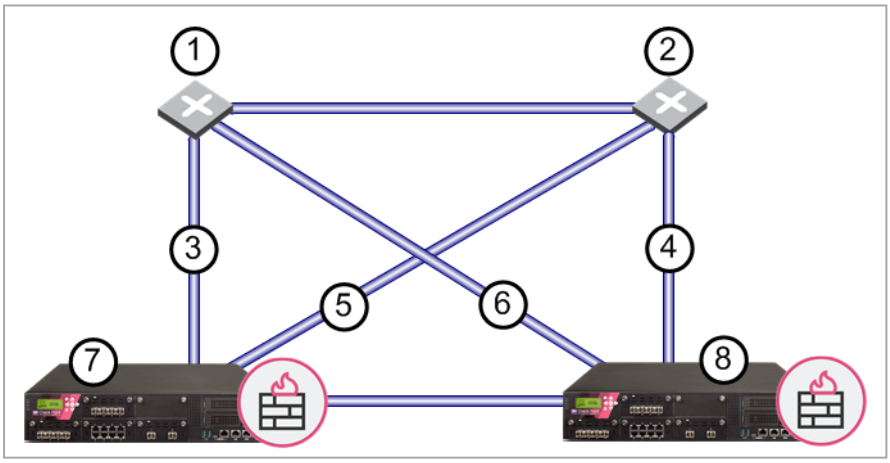
Bonding High Availability failover occurs in one of these cases:

- An active interface detects a link state failure in a monitored interface.
- ClusterXL detects a failure in sending or receiving Cluster Control Protocol (CCP) keep-alive packets.

Fully Meshed Redundancy through Interface Bonding

The Link Aggregation High Availability mode, when deployed with ClusterXL, enables a higher level of reliability by providing granular redundancy in the network.

This granular redundancy is achieved by using a fully meshed topology, which provides for independent backups for both NICs and switches.



Item	Description		Item	Description
1	Switch 1		5	Network connection 2
2	Switch 2		6	Network connection 3
3	Network connection 1		7	VSX Cluster Member 1
4	Network connection 4		8	VSX Cluster Member 2

In this scenario - VSX Cluster Members 1 and 2 are configured in the High Availability mode.

Link Aggregation Load Sharing

Load Sharing provides the ability to spread traffic over multiple subordinate interfaces, in addition to providing interface redundancy.

All interfaces are always active.

Traffic is balanced between interfaces in a manner similar to the way load sharing balances traffic between VSX Cluster Members.

Link Aggregation Load Sharing operates according to either the IEEE 802.3ad or the XOR standard.

In Load Sharing mode, each individual connection is assigned to a specific subordinate interface.

For a specific connection, only the designated subordinate interface is active.

If the designated subordinate interface fails, then the traffic fails over to another interface, which also continues to handle its existing traffic.

Bond Interface Limitations

- You can define a maximum of 4096 interfaces on a Gaia server or appliance.

  The total number of bond interfaces in use is the sum of bonds plus the number of subordinate interfaces contained in each bond.
- Up to eight interfaces can be defined in a Link Aggregation deployment for each bond interface.
- Scalable Platforms: After you configure the VSX Gateway object in the Traditional VSX mode, it is not supported to configure Bond interfaces on the Management ports of a Security Group.

Configuring Bond High Availability Mode

This section explains how to configure High Availability on a bond interface.

Run the CLI commands from the VSX Gateway (VS0) context.

In a VSX Cluster, run these commands on each VSX Cluster Member.

Use the "`active-backup`" value for the "`mode`" parameter to configure High Availability.

Configuring the High Availability Bond

This is a workflow of CLI commands to configure Link Aggregation in High Availability mode.

Notes:

- For exact commands, see *R82 Gaia Administration Guide*.
- When you are enslaving configured interfaces, make sure that these interfaces are not used in other configurations and that IP addresses are not assigned to them.

To configure the Link Aggregation in High Availability mode:

1. Add the bonding group.
2. Add subordinate interfaces to the bonding group.
3. Make sure that the bond is configured correctly.
4. Open SmartConsole and configure the cluster object.
   - For a new Link Aggregation installation, create a new cluster object.
   - For updating an existing configuration, update the interface topology.

Updating the Interface Topology

When you are updating an existing configuration to Link Aggregation, it is necessary to reconfigure the applicable objects to connect to the newly created bond. This includes Virtual Systems, Virtual Routers and Virtual Switches. You can perform these actions in SmartConsole. In most cases, these definitions can be found in the object **Properties** window.

For large existing VSX deployments containing many Domain Management Servers and Virtual Devices, use the "`vsx_util change_interfaces`" command on the Management Server to reconfigure existing object topologies. For example, in a Multi-Domain Server deployment with 200 Domains, each with many Virtual Devices, it is faster to use the "`vsx_util change_interfaces`" command. This command automatically replaces the interface with the new bond on all applicable objects.

Reconfiguring the Bond

To configure the newly created bond for a cluster:

1. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages the VSX Cluster.
2. Delete the subordinate interfaces from the bond that you are not using.
    a. From the navigation tree, click **Topology**.
    b. From the navigation tree, click **Physical Interfaces**.
    c. Select the subordinate interface, and click **Remove**.
    d. Click **OK**.
    e. Do these steps again for all the subordinate interfaces.
3. From Gaia Clish on each VSX Cluster Member, create the new bond interface.
4. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages the VSX Cluster.
5. From the **Gateways & Servers**view or Object Explorer, double-click the VSX Cluster object.
6. From the left navigation tree, click **Physical Interfaces**.
7. Click **Add**, and configure the bond interface.

    The **Physical Interface Properties** window opens.
    a. Enter the bond name.
    b. If the bond is a VLAN trunk, select **VLAN Trunk**.
    c. Click **OK**.
8. From the left navigation tree, click **Topology**.
9. Do these steps for each interface that you are adding to the bond:
    a. Double-click the interface.

        The **Interface Properties** window opens.
    b. From **Interface**, select the bond interface.
    c. Click **OK**.
10. Install the VSX Policy (*<Name of VSX Cluster Object>_VSX*) on the VSX Cluster object.

Reconfiguring Topology with 'vsx_util change_interfaces'

Important - In a Multi-Domain Server environment, all Domain Management Servers must be unlocked in order for this operation to succeed. Meaning, you need to disconnect all SmartConsole clients from all Domain Management Servers.

To reconfigure objects with the "vsx_util change_interfaces" command:

1. Close SmartConsole windows for the Security Management Server and all Domain Management Servers that use the designated interface.
2. Connect to the command line on the Management Server.
3. Log in to the Expert mode..
4. Run the "`vsx_util change_interfaces`" command and follow the on-screen instructions:
    a. Enter the IP address of the Security Management Server or Main Domain Management Server.
    b. Enter the management administrator name and password.
    c. Select VSX Cluster object.
    d. Select **Apply changes to the management database and to the VSX Gateway/Cluster members immediately**.
    e. When prompted, select the interface to be replaced.
    f. When prompted, select the replacement bond interface.
    g. If you wish to replace additional interfaces, enter "**y**" when prompted and repeat the above steps.
    h. To complete the process, enter "**n**".

Configuring Bond Load Sharing Mode

This section explains how to configure Load Sharing on a bond interface.

Run the CLI commands from the VSX Gateway (VS0) context.

In a VSX Cluster configuration, run these commands on each VSX Cluster Member.

Configure one of these Load Sharing modes for the bond interface:

- **Round Robin** - Selects the Active subordinate interfaces sequentially.
- **802.3ad** - Dynamically uses Active subordinate interfaces to share the traffic load. This mode uses the LACP protocol, which fully monitors the interface link between the Check Point Security Gateway and a switch.
- **XOR** - All subordinate interfaces in the UP state are Active for Load Sharing. Traffic is assigned to Active subordinate interfaces based on the transmit hash policy: Layer 2 information (XOR of hardware MAC addresses), or Layer 3+4 information (IP addresses and Ports).

Configuring the Load Sharing Bond

This is a workflow of CLI commands to configure Link Aggregation in Load Sharing mode.

Notes:

- For exact commands, see *R82 Gaia Administration Guide*.
- When you are enslaving configured interfaces, make sure that these interfaces are not used in other configurations and that IP addresses are not assigned to them.

To configure the Link Aggregation in Load Sharing mode:

1. Add the bonding group.
2. Add subordinate interfaces to the bonding group.
3. Define the number of critical interfaces.
4. For configurations that use Performance Pack, configure the core affinities.
5. Make sure that the bond is configured correctly.
6. Open SmartConsole and configure the VSX Cluster object.
   - For a new Link Aggregation installation, create a new cluster object.
   - For updating an existing configuration, update the interface topology.

Setting Critical Required Interfaces

Note - The Critical Required Interfaces feature is supported for ClusterXL only.

A Bond in Load Sharing mode is considered to be down when fewer than a critical minimum number of subordinate interfaces remain up. When not explicitly defined, the critical minimum number of subordinate interfaces, which must remain up, in a bond of **n** interfaces is **n-1**. Failure of an additional subordinate interface (when **n-2** subordinate interfaces remain up) will cause the entire bond interface to be considered down, even if the bond contains more than two subordinate interfaces.

If a smaller number of subordinate interfaces will be able to handle the expected traffic, you can increase redundancy by explicitly defining the critical minimum number of subordinate interfaces. Divide your maximum expected traffic speed by the speed of your subordinate interfaces and round up to a whole number to determine an appropriate number of critical subordinate interfaces.

To define the critical number of subordinate interfaces explicitly, create and edit the following file:

`$FWDIR/conf/cpha_bond_ls_config.conf`

Each line of the file should be written in the following syntax:

```
<Name of Bond> <Critical Minimum Number of Subordinate Interfaces>
```

For example, if `bond0` has 7 subordinate interfaces, and `bond1` has 6 subordinate interfaces, file contents could be:

```
bond0 5
bond1 3
```

In this example:

- `bond0` would be considered down when 3 of its subordinate interfaces have failed.
- `bond1` would be considered down when 4 of its subordinate interfaces have failed.

Affinities of Bond Subordinate Interfaces to CPU Cores

For optimal performance, follow these guidelines:

1. Configure static affinities of bond subordinate interfaces to CPU Cores.
2. Whenever possible, dedicate one processing core to each interface.

3. If there are more physical interfaces than CPU cores, then some CPU cores handle two or more interfaces.

   Use pairs of subordinate interface of the same position with internal and external bonds.

   a. To view positions of subordinate interface in a bond, run in the Expert mode:

      ```
      cat /proc/net/bonding/<Name of Bond Interface>
      ```

   b. Note the sequence of the interfaces in the output.

      Compare this sequence for the two bonds (external bond and its respective internal bond).

      Subordinate interfaces that appear in the same position in the two bonds are interface pairs.

      Set these pairs to be handled by one processing CPU core.

   Example configuration

   An appliance has:

   - Four processing CPU cores:

     core 0, core 1, core 2, and core 3

   - Two bond interfaces:

     `bond0` with subordinate interfaces `eth0`, `eth1`, and `eth2`

     `bond1` with subordinate interfaces `eth3`, `eth4`, and `eth5`

   In such case, two of the CPU cores need to handle two subordinate interfaces each.

   An optimal configuration can be:

CPU core	bond0	bond1
0	eth0	eth3
1	eth1	eth4
2	eth2	
3		eth5

For more information, see the *R82 Performance Tuning Administration Guide*:

- Chapter *CoreXL* > Section *Configuring Affinity Settings*.
- Chapter *CoreXL* > Section *Affinity Settings for 16000 and 26000 Appliances*.

Bond Failover

Either of the following failure scenarios can induce bond failover:

- An active interface detects a link state failure in another monitored interface
- ClusterXL detects a failure in sending or receiving Cluster Control Protocol (CCP) keep-alive packets

Either of these occurrences will induce a failover, either to another subordinate interface within the bond, or between VSX Cluster Members, depending on the circumstances.

Note - The bond failover operation requires a network interface card that supports the Media-Independent Interface (MII) standard.

Link State Initiated Failover

Link-state initiated failover occurs in this sequence:

1. The active subordinate interface detects a **down** link state.
2. The bond initiates failover to a standby interface. Since this is a failover within the bond, the status of the other VSX Cluster Member is unaffected.

   When the number of available subordinate interfaces is fewer than the critical minimum number of interfaces, failover to other VSX Cluster Members occurs (see *"Setting Critical Required Interfaces" on page 248*).
3. If the standby interface continues to detect a link failure, and the initial interface is still down, failover to other VSX Cluster Members occurs.

Failover Initiated by Cluster Control Protocol (CCP)

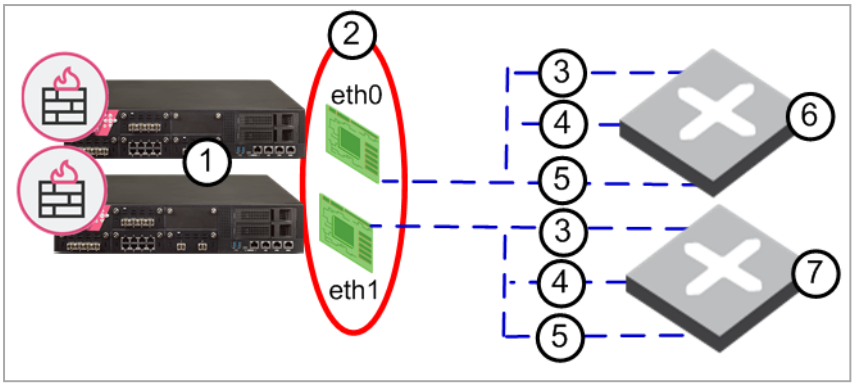
CCP failover occurs only when other VSX Cluster Members are not down, in this sequence.

1. ClusterXL detects a problem sending or receiving of CCP packets.
2. ClusterXL initiates an internal bond failover.
3. ClusterXL monitors CCP packet transmission and reception. If additional problems are detected within three minutes, the system initiates a failover to another VSX Cluster Member.

Failover Support for VLANs

ClusterXL monitors VLAN IDs for connectivity failure or miscommunication, and initiates failover when necessary. By default, both the highest and the lowest VLAN IDs are monitored for failure. This is done by sending ClusterXL Control Protocol (CCP) packets on round-trip paths at a set interval.

You can configure VSX to monitor all VLANs.



Item	Description		Item	Description
1	Cluster		5	VLAN 3
2	bond 0		6	S-1
3	VLAN 1		7	S-2
4	VLAN 2			

When a failure is detected, a log of the failure is recorded in the **Logs & Events** view.

Monitoring the Highest and Lowest VLAN IDs

By default, the highest and lowest VLAN IDs indicate the status of the physical connection. These VLAN IDs are always monitored and a connectivity failure in either initiates a failover. In most deployments this is the desired setting, as it supports the primary purpose of the feature (detecting a connectivity failure) and the traffic generated on the network is light. However, this setting only detects VLAN configuration problems on the switch for the highest and lowest VLAN IDs.

Configuring Cisco Switches for Link Aggregation Load Sharing Mode

These are sample configuration commands for Cisco switches (for the exact commands, refer to the Cisco documentation for your switch model and the switch operating system version).

For 802.3ad (LACP)

```
Switch# conf t
Switch(config)# port-channel load-balance src-dst-ip
Switch(config)# interface FastEthernet <all the participating
ports>
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# channel-protocol lacp
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# switchport access vlan <desired vlan number>
Switch(config-if)# end
Switch# write
```

For XOR

```
Switch# conf t
Switch(config)# port-channel load-balance src-dst-ip
Switch(config)# interface FastEthernet <all the participating
ports>
Switch(config-if)# channel-group 1 mode on
Switch(config-if)# exit
Switch (config)# interface port-channel 1
Switch(config-if)# switchport access vlan <desired vlan number>
Switch(config-if)# end
Switch# write
```

Troubleshooting Bonded Interfaces

Troubleshooting Workflow

1. Connect to the command line.
2. Log in to the Expert mode.
3. Check the status of the bond:

   ```
   cat /proc/net/bonding/<bond id>
   ```
4. If there is a problem, check if the physical link is down, as follows:
   a. Execute the following command:
      - In Gaia Clish:

        ```
        show cluster bond name <bond_name>
        ```
      - In the Expert mode:

        ```
        cphaprob show_bond <bond_name>
        ```

   b. Look for a subordinate interface that reports the status of the `link` as *no*.
   c. Check the cable connections and other hardware.
   d. Check the port configuration on the switch.
5. Check if a VSX Cluster Member is down, by running:
   - In Gaia Clish:

     ```
     show cluster state
     ```
   - In the Expert mode:

     ```
     cphaprob state
     ```

   If any of the VSX Cluster Members has a `State` other than *Active*, see the *R82 ClusterXL Administration Guide* - Chapter *Monitoring and Troubleshooting Clusters*.

On a VSX Cluster Member, reboot is needed after the following actions on a bond interface:

1. Changing a bond mode.
2. Adding a subordinate interface into a bond

Note - Removing a subordinate interface does not require reboot.

For further information regarding bond status and failovers, view logs in the **Logs & Events** view. Any interface bond status change is logged and can be viewed in **Logs & Events**.

Connectivity Delays on Switches

When using certain switches, connectivity delays may occur during some internal bond failovers. With the various features that are now included on some switches, it can take close to a minute for a switch to begin servicing a newly connected interface. The following are suggestions for reducing the startup time after link failure.

1. Disable auto-negotiation on the applicable interface.
2. On some Cisco switches, enable PortFast, as detailed below.

   Note - PortFast is not applicable if the bond group on the switch is configured as Trunk.

Warning Regarding Use of PortFast

The PortFast feature should never be used on ports that connect to other switches or hubs. It is important that the Spanning Tree complete the initialization procedure in these situations.

Otherwise, these connections may cause physical loops where packets are continuously forwarded (or even multiply) in such a way that network will ultimately fail.

Sample Configuration of PortFast on a Cisco Switch

The following are the commands necessary to enable PortFast on a Gigabit Ethernet 1/0/15 interface of a Cisco 3750 switch running IOS.

1. Enter configuration mode:

   ```
   cisco-3750A# conf t
   ```

2. Specify the interface to configure:

   ```
   cisco-3750A(config)# interface gigabitethernet1/0/15
   ```

3. Set PortFast on this interface:

   ```
   cisco-3750A(config-if)# spanning-tree portfast
   ```

Optimizing VSX

This section describes different features that let you monitor and optimize the VSX performance.

Monitoring Memory Resources (vsx mstat)

Use the *"vsx mstat" on page 311* command to monitor the memory the VSX Gateway uses.

The command shows an overview of the memory that the system and each Virtual Device is using.

These are the global memory resources that are shown:

- **Memory Total** - Total physical memory on the VSX Gateway.
- **Memory Free** - Available physical memory.
- **Swap Total** - Total of swap memory.
- **Swap Free** - Available swap memory.
- **Swap-in rate** - Total memory swaps per second.

The Virtual Devices are listed according to the VSIDs.

Run the "`vsx stat -v`" command to show the VSID for the Virtual Devices.

You must be in the Expert mode to run this command.

In addition:

1. Run the `cpview` command in the context of Virtual System 0 (see *"cpview" on page 299*).
2. From the top, click:

   Advanced > VSX > VSs > Physical-Resources

   Note - This tab shows the memory consumption by Virtual Systems and by Virtual Routers.

Monitoring CPU Resources

From R80.40, the CPU Resource Control is integrated into the CPView utility.

1. Go to the context of Virtual System 0:
   - In the Expert mode:

     ```
     vsenv
     ```

   - In Gaia Clish:

     ```
     set virtual-system 0
     ```

2. Run the CPView:

   ```
   cpview
   ```

   See *"cpview" on page 299*.

3. From the top, click:

   Advanced > VSX > VSs > Physical-Resources

   Notes:
   - This tab shows the CPU consumption by Virtual Systems and by Virtual Routers.
   - The "**CPU %**" column shows the percentage of CPU used by all the processes of each Virtual System.
     The column shows a percentage of a single CPU (the same behavior as in the "`top`" command).
     Example:
     - There are 4 CPU cores on the VSX Gateway.
     - The processes of the Virtual System "VS1" are using:
       - 30% of CPU 0
       - 40% of CPU 1
       - 50% of CPU 2
       - 10% of CPU 3

     In such case, the "**CPU %**" column shows 130% for VS1.
   - To get the CPU usage for the VSX Gateway / VSX Cluster Member, divide the "**CPU %**" value in the **Total Resource Consumption** section by the number of the CPU cores.

SNMP Monitoring

In This Section:

Supported SNMP Versions 258
Supported SNMP Modes 258
SNMP Default Mode 259
SNMP VS Mode 260
SNMP VS in the "vs-direct-access" Mode 261
Configuring SNMP Modes 262
Example SNMP queries for Virtual Systems 264
The VSX SNMP Tree 267

For more about using SNMP, see:

- *R82 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*
- sk90860: How to configure SNMP on Gaia OS

Supported SNMP Versions

SNMP v1, v2c, and v3 are supported in all monitor modes.

Note - For SNMP queries of Virtual Devices using the VS0 IP address:

- **SNMP v1 and v2c**
  Query the Virtual Device using the VSID and the configured SNMP community.
- **SNMP v3**
  Query the virtual device using the VSID and SNMP v3 context mechanism.

Supported SNMP Modes

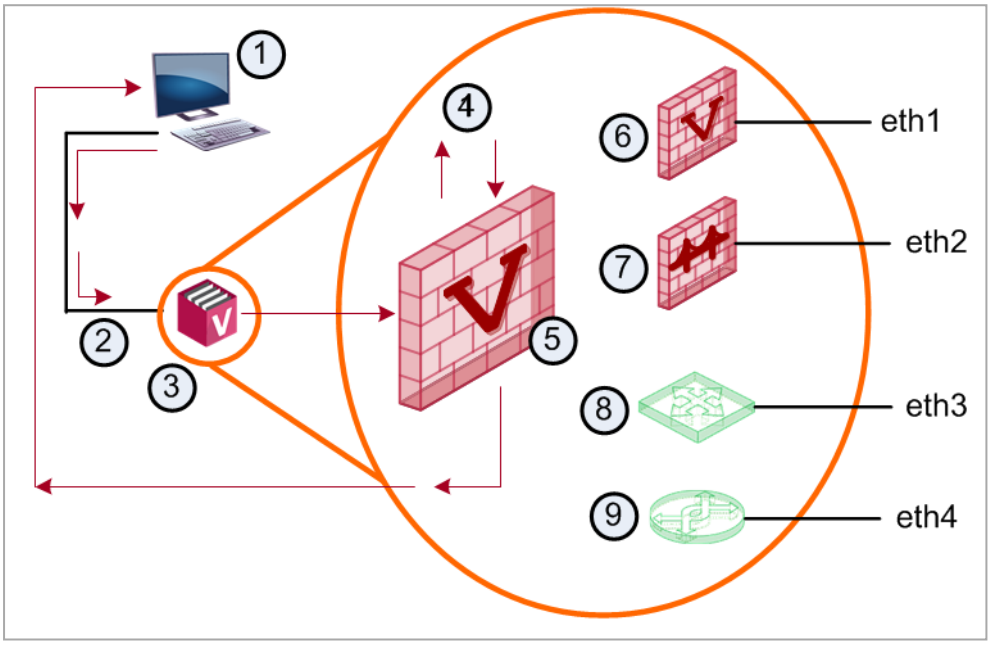
VSX supports these SNMP modes:

- SNMP Default Mode
- SNMP VS Mode
- SNMP VS in *vs-direct access* mode

SNMP Default Mode

In SNMP default mode:

- The SNMP daemon runs only in the context of VS0 (the VSX Gateway).
- The VS0 SNMP daemon has a set of tables with counters (VSX SNMP tree) for each Virtual Device.
- SNMP queries must be sent to IP address of the VSX Gateway (context is VS0).



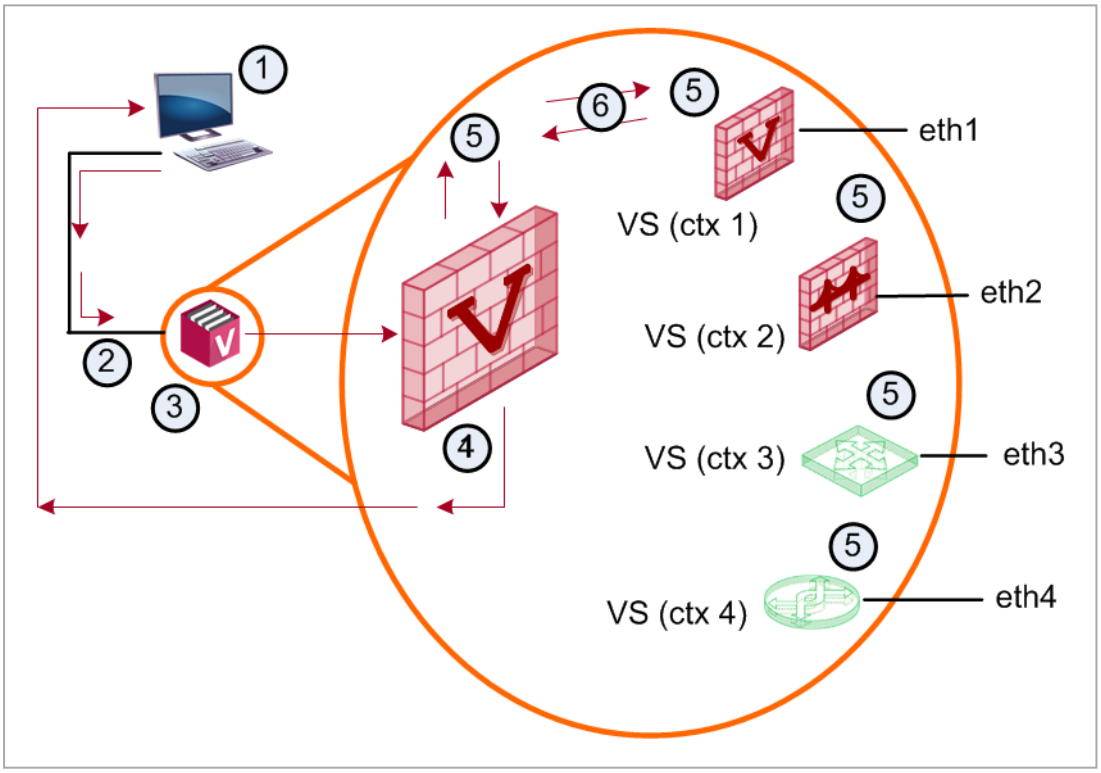
Item	Description		Item	Description
1	SNMP Server that sends SNMP Requests to VSX Gateway		6	Virtual System 1 (ctx 1)
2	eth0		7	Virtual System in Bridge mode (ctx 2)
3	VSX Gateway		8	Virtual Router (ctx 3)
4	SNMP Daemon		9	Virtual Switch (ctx 4)
5	Virtual System 0			

SNMP VS Mode

In SNMP VS mode:

- Each Virtual Device has separate SNMP daemon running in the context of that Virtual Device.
- Query for Virtual Devices uses the VS0 IP address.
- You must run the SNMP query using the interface on the VSX Gateway.
  - The query is relayed to the specified Virtual Device.
  - The Virtual Device sends the response through the same VSX Gateway interface.
- The VS ID must be specified in the SNMP query.

Note - Default mode query functionality is not decreased when you enable SNMP VS mode.

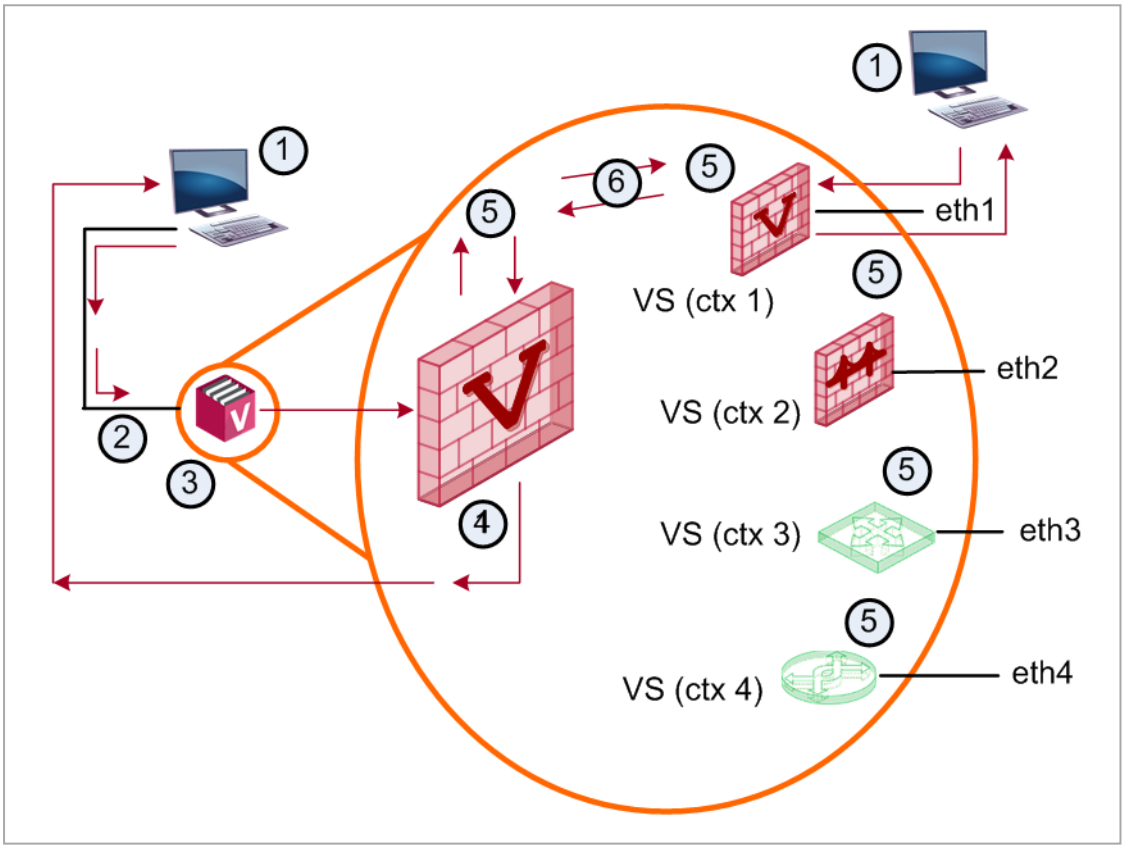


Item	Description		Item	Description
1	Query Host		4	VS 0
2	eth0		5	SNMP Daemon
3	VSX Gateway		6	UDS

SNMP VS in the "vs-direct-access" Mode

- SNMP VS in the `vs-direct-access` mode is available only when the SNMP VS mode is enabled.
- Enables SNMP queries on the IP address of a Virtual System (not only VS0), or Virtual Router.

Notes:
- For cluster deployments, you can query only Virtual IP addresses.
- Only Virtual Devices with an IP address can be queried, not Virtual Switches or Virtual Bridges.



Item	Description		Item	Description
1	Query Host		4	VS 0
2	eth0		5	SNMP Daemon
3	VSX Gateway		6	UDS

Configuring SNMP Modes

Each Virtual System must meet these requirements:

SNMP USM user

- To use SNMP v3 queries, an SNMP USM user must be defined.

  For more on USM user creation commands, see the *R82 Gaia Administration Guide*.

- To use SNMP v3 queries on VSX, the USM user must be configured with the allowed Virtual Devices:

  ```
  set snmp usm user <User_Name> vsid <VSID>
  ```

- By default, a USM user in VSX has no allowed Virtual Devices.

Allowed interfaces

If you enable the *vs-direct-access mode*, the Virtual System accepts SNMP queries on all the interfaces.

To prevent SNMP queries for a specified interface, add a new rule to the policy that blocks SNMP traffic on that interface.

Query source

In the *vs mode* and the *vs-direct-access mode*, there is no specification for query source.

All sources allowed in the Security Policy are valid.

Running SNMP Queries

When you query a Virtual System Load Sharing cluster with the VSX Cluster Member (VS 0) Virtual IP address, the Virtual System on the Active VSX Cluster Member (VS 0) replies to the query.

An Active Virtual System on a Standby VSX Cluster Member does not reply to the query.

If you want to query the Active Virtual System on a Standby VSX Cluster Member, use the real IP address of the VSX Cluster Member.

SNMP Configuration

See the *R82 Gaia Administration Guide* and *sk90860: How to configure SNMP on Gaia OS*.

To Configure	Run
SNMP Default	1. `set snmp agent on` 2. `set snmp mode default`
SNMP mode VS	1. `set snmp agent on` 2. `set snmp mode vs`
SNMP direct-vs-access	1. `set snmp agent on` 2. `set snmp mode vs` 3. `set snmp vs-direct-access on`

Example SNMP queries for Virtual Systems

This section shows example SNMP queries.

To run an SNMP v3 query using the VSX (VS 0) IP address

In Gaia Clish:

1. Enable the SNMP agent for context VS:

```
set snmp agent on
```

2. Add an SNMP user with permissions for VSs 2,15:

```
add snmp usm user admin security-level authNoPriv auth-pass-
phrase abcd1234
set snmp usm user admin vsid 2,15
```

3. Set SNMP VS mode:

```
set snmp mode vs
```

4. Send the remote queries, where:

   - `vsidN` is the SNMP context name required by SNMP v3.
   - The IP address is the management IP address of the VSX Gateway or VSX Cluster.

   For example (in the Expert mode):

```
snmpwalk -n vsid2 -v 3 -l authNoPriv -u admin -A abcd1234
192.0.2.5 ifDesc
snmpwalk -n vsid15 -v 3 -l authNoPriv -u admin -A abcd1234
192.0.2.5 sysName
```

   192.0.2.5 is the IP address of the Management Server.

To run an SNMP v1/v2c query using the VSX (VS 0) IP Address

In Gaia Clish:

1. Enable the SNMP agent for context VS 0:

```
set snmp agent on
```

2. Enable SNMP v1/v2:

```
set snmp agent-version any
```

3. Set the SNMP community:

```
set snmp community public read-only
set snmp community private read-write
```

4. Set the SNMP mode to VS:

```
set snmp mode vs
```

5. Send remote queries, where:

   - The community has the VSID or Virtual System name as a suffix.
   - The IP address is the Management IP address of the VSX Gateway or VSX Cluster.

   For example, to query a Virtual System with the name "MY_VS" or has VSID "2", run

   In the Expert mode, run:

```
snmpwalk -v 1 -c public_2 192.0.2.5 ifDescr
snmpwalk -v 1 -c private_MY_VS 192.0.2.5 ifDescr
```

Communities with suffixes are created automatically.

Community name collisions might occur in special cases, for example if we use these communities:

- Read-only community = `private`
- Read-write community = `private_1`

The communities' `private_1` and `private_1_1` are automatically created for VSID 1.

`Private_1` is not a unique community. The community is ambiguous and using it results in unexpected behavior.

To run an SNMP query using the Virtual Device's IP address

1. Enable the SNMP agent for context VS0:

```
set snmp agent on
```

2. Add an SNMP user:

```
add snmp usm user admin security-level authNoPriv auth-pass-
phrase abcd1234
```

3. Specify USM user permissions for Virtual Devices:

```
set snmp usm user admin vsid 0-10
```

4. Set the SNMP community:

```
set snmp community public read-only
set snmp community private read-write
```

5. Set SNMP VS mode:

```
set snmp mode vs
```

6. Enable SNMP queries over Virtual Device's interfaces:

```
set snmp vs-direct-access on
```

7. Send remote queries, where the IP address is the Virtual IP address of the Virtual Device.

   In the Expert mode, run:

```
snmpwalk -v 1 -c public 192.0.2.81 ifDescr
snmpwalk -v 2c -c public 192.0.2.81 ifDescr
snmpwalk -v 1 -c private 192.0.2.82 ifDescr
snmpwalk -v 2c -c private 192.0.2.82 ifDescr
snmpwalk -v 3 -l authNoPriv -u admin -A abcd1234 192.0.2.83
ifDescr
```

Notes:

- The SNMP community used in the queries is the same community that you configured earlier.
- Only the active Virtual Device is queried.

Important - SNMP traps are available only for VS 0

The VSX SNMP Tree

To get information from a Virtual Device (Virtual System, Virtual Switch, or Virtual Router), you must load the Check Point MIB file into your SNMP Browser.

- The MIB file on the VSX Gateway (context of VS 0) is:
  `$CPDIR/lib/snmp/chkpnt.mib`
- The VSX OID is: `.1.3.6.1.4.1.2620.1.16`

Example commands in the Expert mode:

- To run an SNMP v2c query for VSX status table, run:

```
snmpwalk -m $CPDIR/lib/snmp/chkpnt.mib -c public -v 2c
192.0.2.83 vsxStatusTable
```

- To run an SNMP v3 query for the VSX memory usage table, run:

```
snmpwalk -m $CPDIR/lib/snmp/chkpnt.mib -v 3 -l authNoPriv -u
admin -A abcd1234 192.0.2.83 vsxStatusMemoryUsageTable
```

The vsxCountersTable refresh time:

The `vsxCountersTable` refresh time is configured in this file:

`$FWDIR/conf/amon_vsx_refresh_interval`

The default value is 30 (seconds).

Configuring Jumbo Frames

VSX supports Jumbo Frames and lets you configure up to the maximum MTU of the NIC driver.

Jumbo Frames on a Virtual Switch

Configure the MTU of a Virtual Switch to enable Jumbo Frames on the Virtual Systems that are connected to the Virtual Switch. When you configure the MTU of the Virtual Switch, all the related Warp Links and interfaces are automatically changed to the new value.

You cannot configure the MTU of a Warp Link from the Virtual System.

To configure Jumbo Frames on a Virtual Switch:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual Switch.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Virtual Switch object.
4. From the left tree, click **Topology**.
5. In the **Interfaces** section, select the applicable interface and click **Edit**.
6. On the **General** tab, configure the **MTU**.
7. Click **OK**.
8. Publish the SmartConsole session.

Jumbo Frames on a Virtual Router

Configure the MTU of a Virtual Router to enable Jumbo Frames on the interfaces. To change the MTU of Warp Links, configure the settings of the Virtual System.

To configure Jumbo Frames on a Virtual Router:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual Router.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Virtual Router object.
4. From the left tree, click **Topology**.
5. In the **Interfaces** section, select the applicable interface and click **Edit**.
6. On the **General** tab, configure the **MTU**.
7. Click **OK**.
8. Publish the SmartConsole session.
9. Install the applicable Access Control policy on the Virtual Router object.

Jumbo Frames on a Virtual System in Bridge Mode

Configure the MTU of a Virtual System in Bridge Mode to enable Jumbo Frames on the interfaces.

To configure Jumbo Frames on a Virtual System in Bridge Mode:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual System.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Virtual System object.
4. From the left tree, click **Topology**.
5. In the **Interfaces** section, select the applicable interface and click **Edit**.
6. On the **General** tab, configure the **MTU**.
7. Click **OK**.
8. Publish the SmartConsole session.
9. Install the applicable Access Control policy on the Virtual System object.

Bridge Mode

By implementing native Layer 2 bridging instead of IP routing, you can add Virtual Systems without adversely affecting the existing IP structure.

When in the Bridge mode, Virtual System interfaces do not require IP addresses.

You can optionally assign an IP address to the Virtual System itself (not the interfaces) to enable Layer 3 monitoring, which provides network fault detection functionality.

VSX supports these Bridge mode models:

- **Active/Active Bridge Mode**: Provides redundancy while preventing undesirable loops between redundant switches.
- **Active/Standby Bridge Mode**: Provides path redundancy and loop prevention, while offering seamless support for Virtual System Load Sharing and overcoming many of the limitations of STP.

Active/Active Bridge Mode (Spanning Tree Protocol)

The Spanning Tree Protocol is an industry standard technology to prevent loops in high-speed switched networks.

To use the STP Bridge mode, you must have STP deployed and properly configured on your network.

These STP Layer 2 protocols are supported:

- 802.1d
- 802.1q
- 802.1s
- 802.1w
- PVST+

See your vendor documentation to learn how to deploy and configure STP on your network hardware.

Active/Standby Bridge Mode

The Active/Standby Bridge Mode enhances both:

- *High Availability* (for significant improvements).
- *Virtual System Load Sharing* (VSLS) in VSX Cluster environments (for throughput distributed among Virtual Systems).

Active/Standby Bridge Mode has these advantages:

- Instantaneous failover.
- Enhanced administrator control over bridge failover.
- VSLS support.
- VLAN translation.

The principal limitation of the Active/Standby Bridge Mode is that it breaks the STP tree structure.

Note - When configuring a Virtual System in the Active/Standby Bridge Mode, you should remove Virtual System VLANs from the STP database in the switches. This action prevents delays due to trunk interface failback.

Three Layer Hierarchical Model

A three-layer hierarchical model is used in large, high-traffic network environments.

1. A **core network**, with high-speed backbone switches that direct traffic to and from the Internet and other external networks.
2. A **distribution layer**, with routers, for connectivity between the core and the access layer.
3. An **access layer**, with redundant LAN switches, that forward traffic to and from internal networks.

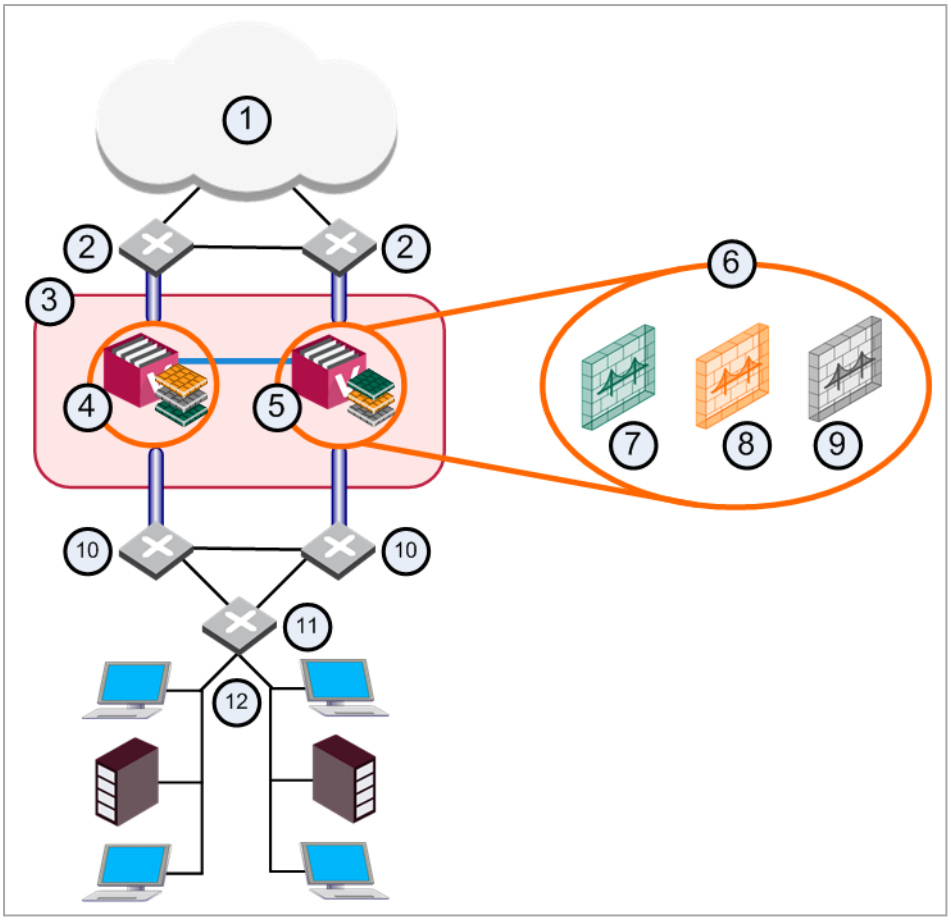
VSX in Active/Standby Bridge Mode is incorporated in the **distribution** layer, enforcing the security policy.

The routers direct external traffic to the appropriate Virtual System through a segregated VLAN. Inspected traffic exits the Virtual System through a separate segregated VLAN, to the routers and then to internal destinations.

VLAN Shared Interface Deployment

In this deployment, which cannot function using a standard STP Bridge mode configuration, each VSX Cluster Member connects to pair of redundant switches through a VLAN Trunk.

All Virtual Systems in a given VSX Cluster Member share the same VLAN Trunk.



Item	Description		Item	Description
1	Internet		9	Virtual System 3 is Backup
2	Redundant switches (external)		10	Redundant switches (internal)
3	VSX Cluster		11	VLAN Switch
4	VSX Cluster Member 1		12	Internal Networks
5	VSX Cluster Member 2			Sync Network
6	Virtual Systems in Bridge Mode			Physical Interface
7	Virtual System 1 is Active			VLAN Trunk
8	Virtual System 2 is Standby			

With Active/Standby Bridge Mode in High Availability mode, VSX Cluster directs traffic to VSX Cluster Members according to administrator-defined priorities and status.

In Virtual System Load Sharing deployments, the system distributes the traffic load amongst VSX Cluster Members according to the Virtual System Load Sharing configuration.

Virtual System in Bridge Mode

In This Section:

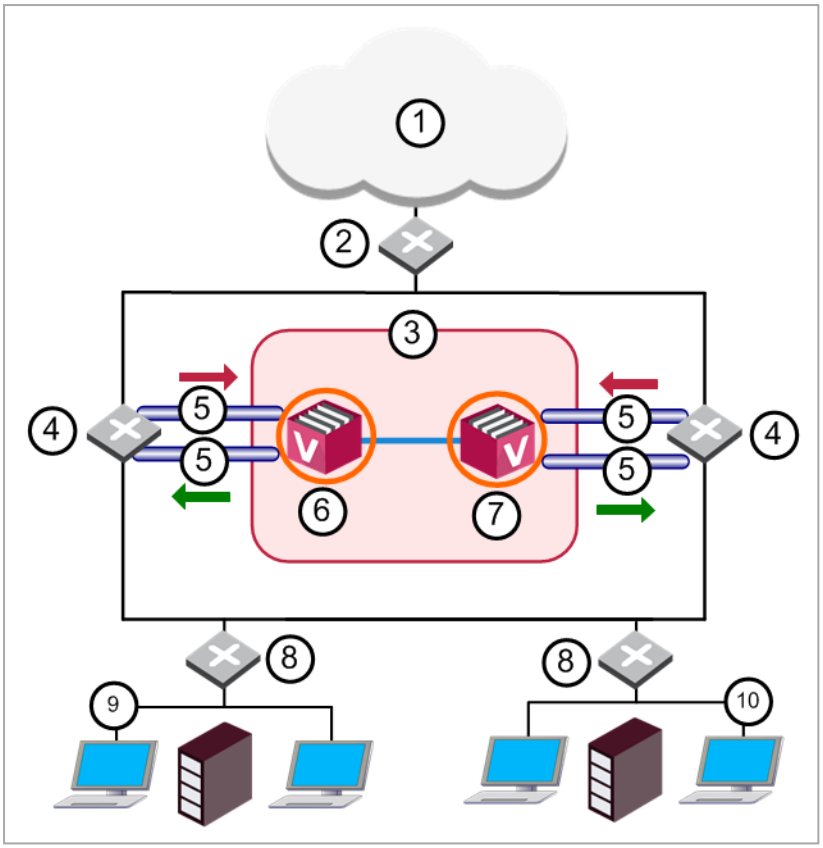
Core Network Security 273
Configuring Virtual Systems for the Active/Standby Bridge Mode 275
Multi Bridge Interfaces 276

Important:

- From R81, it is possible to add bridge interfaces to regular Virtual Systems with the **vsx_provisioning_tool**.
  See *"Adding a Bridge Interface to a Virtual System" on page 382*.
- From R81.10, it is possible to add bridge interfaces to regular Virtual Systems in SmartConsole.
  See *"Configuring Bridge Interfaces in Regular Virtual Systems" on page 116*.

Core Network Security

Many Enterprise environments are based on core networks. Situated adjacent to core network backbone switches, VSX protects the internal network by providing security at Layer 2, Layer 3 or both. VSX communicates with the core network using the existing infrastructure. With Virtual Systems in the Bridge Mode, VSX can protect departmental networks, while simultaneously preventing network segmentation. In this case, switches are located at the entrance to each department's network.



Item	Description		Item	Description
1	Internet		8	LAN Switches
2	Core Network Backbone switch		9	Sales
3	VSX Cluster		10	Finance
4	Router			Sync Network
5	VLAN			Physical Interface
6	Member 1			VLAN Trunk
7	Member 2			

VSX ensures connectivity between the core network and the Internet or external networks, while providing perimeter security.

Security can be configured on a per VLAN basis.

Configuring Virtual Systems for the Active/Standby Bridge Mode

To configure a Virtual System in Bridge Mode, define it as such when you first create the Virtual System object.

Important - You cannot configure an existing non-Bridge Mode Virtual System to work in the Bridge Mode.

To configure a Virtual System for the Active/Standby Bridge Mode:

1. In the **Virtual System General Properties** page of the new Virtual System object, select **Bridge Mode**.
2. Click **Next**.

   The **Virtual System Network Configuration** window opens.
3. Configure the external and internal interfaces for the Virtual System.
4. **Optional:** Select **Enable Layer 3 Bridge Interface Monitoring**.

   The IP address must be unique and on the same subnet as the protected network.
5. Click **Next**.
6. Click **Finish**.

Multi Bridge Interfaces

This feature is supported for:

- VSX Gateways
- VSX Clusters in the Active/Active Bridge Mode
- VSX Clusters in the Active/Standby Bridge Mode

Multi Bridge allows traffic from many different VLANs to move through one Virtual System in the Bridge Mode.

In a Virtual System in the Bridge Mode, you can add physical and VLAN interfaces.

When you add more than two VLAN interfaces, Multi Bridge is automatically enabled.

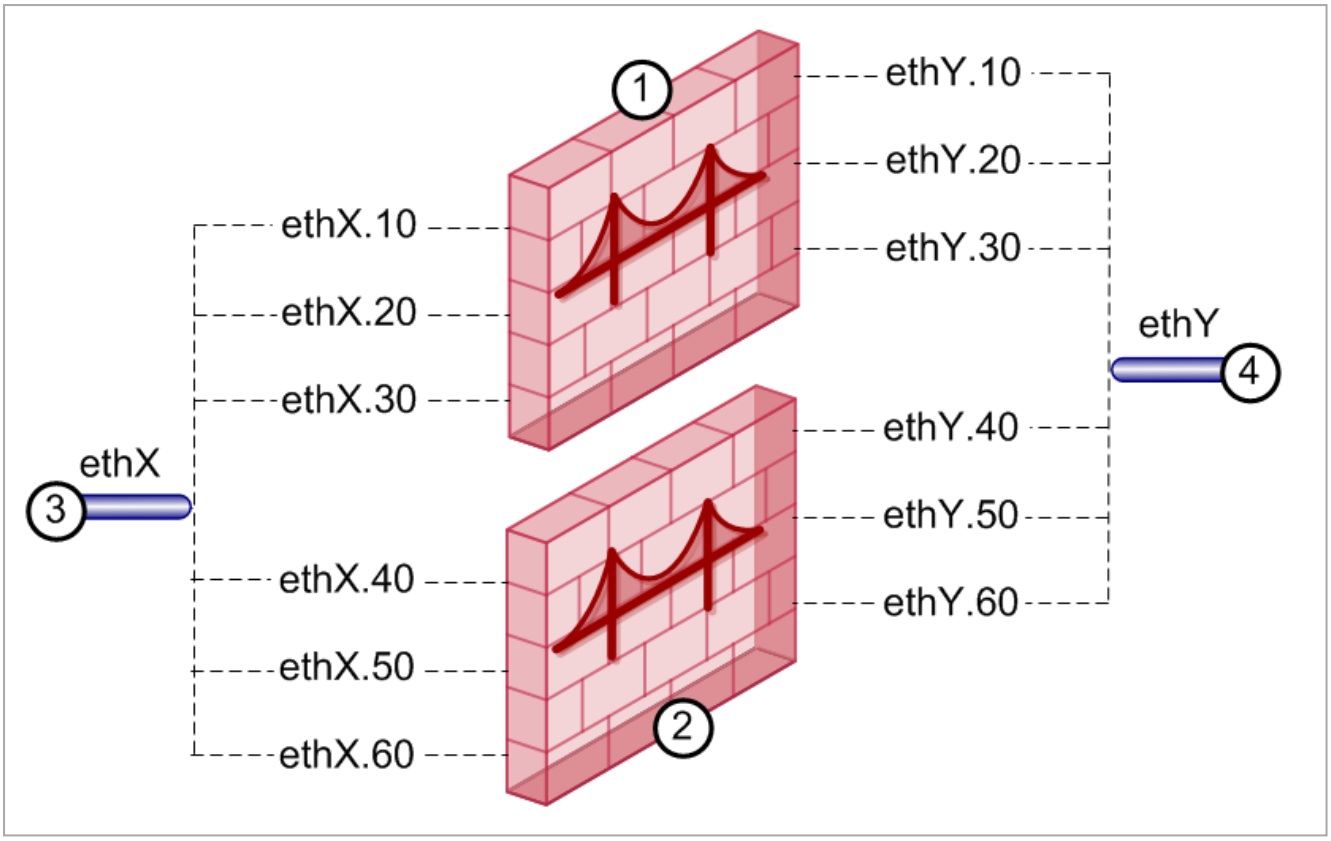
Configure the same VLAN tag on each set of two interfaces to bridge them.

Requirements for Multi Bridge interfaces:

- All interfaces must be VLANs.
- You can make multiple bridges only between two VLAN Trunks.
- You can add up to 64 pairs of VLAN interfaces for one Multi Bridge.
- Those two VLAN Trunks must be used together, and not with other VLAN Trunks, in other Virtual Systems in Bridge Mode or Multi Bridges.

  For example, you define `eth1.10`, `eth2.10`, `eth1.20`, `eth2.20`.

  Now the VLAN Trunks, `eth1` and `eth2`, cannot be used with other VLAN Trunks on other Virtual Systems in Bridge Mode: `eth1.30` cannot bridge with `eth3.30`.



Item	Description
1	Virtual System in Bridge Mode with three bridges on VLAN interfaces with tags 10, 20, and 30.
2	Virtual System in Bridge Mode with three bridges on VLAN interfaces with tags 40, 50, and 60.
3 and 4	VLAN Trunks. Each must be paired with the other in all bridges, or used without bridging. They cannot be paired with a different VLAN Trunk.

Note - Names of Multi Bridge interfaces have a template "`br`*`XXXXXX`*", where "`X`" are digits.

To configure a new Multi Bridge:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the new Virtual System.
2. From the left navigation panel, click **Gateways & Servers**.
3. Create a new Virtual System object in one of these ways:

- From the top toolbar, click the **New (✳) > VSX > New Virtual System**.
- In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > VSX > New Virtual System**.
- In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Virtual System**.

4. In the **Name** field, enter the name for the new Virtual System.
5. In the **VSX Gateway / Cluster** field, select the applicable VSX Gateway or VSX Cluster.
6. Select **Bridge Mode**.
7. Click **Next**.
8. In the **Interfaces** section, click **Add** to add the first VLAN interface for the bridge.
9. In the **Interfaces** section, click **Add** again to add the second VLAN interface for the bridge.
10. In the **Interfaces** section, add more VLAN interface pairs to the Multi Bridge in the same way.

    Make sure the interfaces in each pair have the same VLAN tag, from different interfaces.

    For example:

    ```
    eth2.50,eth2.51
    ```

    ```
    eth3.50,eth3.51
    ```

    Make sure to use the same two VLAN Trunks.
11. Click **Next**.
12. Click **Finish**.
13. Install the applicable Access Control Policy on the new Virtual System object.

To convert a Bridge to a Multi Bridge:

1. Connect with SmartConsole to the Security Management Server or Target Domain Management Server that manages the Virtual System in the Bridge Mode.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Virtual System object.
4. From the left tree, click **Bridge Configuration > Topology**.
5. In the **Interfaces** section, if there are physical interfaces in the **Interfaces** list, remove them.
6. In the **Interfaces** section, add more VLAN interface pairs to the Multi Bridge.
7. Click **OK**.
8. Install the applicable Access Control Policy on the Virtual System object.

VSX Cluster in Bridge Mode

In This Section:

Enabling Active/Standby Bridge Mode on a New VSX Cluster *280*

Enabling Active/Standby Bridge Mode on an Existing VSX Cluster *281*

Enabling Active/Active Bridge Mode on an Existing VSX Cluster *282*

For more information, see the *R82 Installation and Upgrade Guide* > Chapter *Special Scenarios for Security Gateways* > Section *Deploying a Security Gateway or a ClusterXL in Bridge Mode*.

Enabling Active/Standby Bridge Mode on a New VSX Cluster

1. During the Gaia First Time Configuration Wizard of each VSX Cluster Member, on the **Products** page, select **ClusterXL**.
2. After the First Time Configuration Wizard is complete and reboot:
   - If you enabled the **Per Virtual System State** feature (required for VSLS), the Active/Standby Bridge Mode is enabled automatically.
   - If you chose **not** to enable the Virtual System Load Sharing before, then:
     a. Connect to the command line on each VSX Cluster Member.
     b. Run:

     ```
     cpconfig
     ```

     c. Select the option to enable **Active/Standby Bridge Mode**, enter **y**, and continue the configuration.
3. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages this VSX Cluster.
4. From the left navigation panel, click **Gateways & Servers**.
5. Double-click the VSX Cluster object.

   The **VSX Cluster Properties** window opens.
6. From the left tree, click **Other** > **VSX Bridge Configuration**.
7. Select **Check Point ClusterXL**.

   The Active/Standby Bridge Mode loop detection algorithms in ClusterXL are enabled.

8. Click **OK**.
9. Install the VSX Policy on the VSX Cluster object.

   The name of this policy is:

   *<Name of VSX Cluster Object>*_VSX

Enabling Active/Standby Bridge Mode on an Existing VSX Cluster

1. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages the VSX Cluster.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the VSX Cluster object.

   The **VSX Cluster Properties** window opens.
4. From the left tree, click **Other** > **VSX Bridge Configuration**.
5. Select **Check Point ClusterXL**.

   The Active/Standby Bridge Mode loop detection algorithms in ClusterXL are enabled.
6. Click **OK**.
7. Install the VSX Policy on the VSX Cluster object.

   The name of this policy is:

   *<Name of VSX Cluster Object>*_VSX
8. On each VSX Cluster Member:
   a. Connect to the command line.
   b. Log in to the Expert mode.
   c. Run:

      ```
      cpconfig
      ```

   d. Select **Enable ClusterXL for Bridge Active/Standby**.
   e. Exit from the `cpconfig` menu.
   f. Reboot.

Enabling Active/Active Bridge Mode on an Existing VSX Cluster

1. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages the VSX Cluster.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the VSX Cluster object.

   The **VSX Cluster Properties** window opens.
4. From the left tree, click **Other** > **VSX Bridge Configuration**.
5. Select **Standard Layer 2 Loop Detection Protocols**.
6. Click **OK**.
7. Install the VSX Policy on the VSX Cluster object.

   The name of this policy is:

   *<Name of VSX Cluster Object>*_VSX
8. On each VSX Cluster Member:
   a. Connect to the command line.
   b. Log in to the Expert mode.
   c. Run:

      ```
      cpconfig
      ```
   d. Select **Disable ClusterXL for Bridge Active/Standby**.
   e. Exit from the `cpconfig` menu.
   f. Reboot.

VSX Diagnostics and Troubleshooting

This chapter presents basic diagnostic and troubleshooting procedures to follow if you encounter a problem while working with VSX. This diagnostic routine will assist you in determining the source of the problem. This chapter presents several known issues and their solutions.

Most problems are caused by configuration errors occurring during the process of defining VSX Gateway, clusters and/or Virtual Devices. Another common source of problems involves networking and connectivity issues affecting VSX behavior. These problems are listed according to the order in which you will likely encounter them. Before reading and following a certain workaround, make sure you've read all the previous workarounds, and that those steps in the configuration were successful.

In some of the cases, one initial problem can cause problems in later stages of the configuration. For that reason, it is important to find the root of the problem when you are trying to understand what went wrong.

Important - In SmartView Monitor, Firewall History and System History counters do not show data for Virtual Systems.

General Troubleshooting Steps

If you suspect that there is a problem with your VSX configuration, there are several diagnostic procedures that you can follow to determine the source.

These procedures utilize various commands documented in the *"Command Line Reference" on page 292*.

1. Perform a basic configuration check for each VSX Gateway or VSX Cluster Member by running the "`vsx stat -v`" command. The output will allow you to:
    a. Account for all Virtual Systems and make sure that none are missing from the configuration.
    b. Make sure all Virtual Devices are Active
    c. Make sure the correct Security Policy is installed for each Virtual System
    d. Make sure the SIC trust is established with the Management Server
2. Run the "`cplic print`" command on each VSX Gateway, VSX Cluster Member and Management Server to make sure the appropriate licenses are installed.
3. Run the `cphaprob stat` command on each VSX Cluster Member to verify its status. If a member is listed with a status other than **Active**, **Standby**, or **Backup**, refer to the "*Troubleshooting*" chapter in the *R82 ClusterXL Administration Guide* for additional troubleshooting assistance.
4. If you suspect that a Virtual System is experiencing connectivity problems, perform the following steps:
    a. Run the "`vsenv <VSID>`" command to set the context to the appropriate Virtual System.
    b. Run the "`fw getifs`" command to display the interface list for the Virtual System.
    c. Examine connectivity status using standard operating system commands and tools such as: `ping`, `traceroute`, `tcpdump`, `ip route`, `ftp`, and so on. Some of these run according to context (i.e. routing, source and destination IP addresses). .

    You can also execute the "`ip route`" and "`ip link`" commands.

    If these tests indicate that all interfaces and routers have connectivity, and appear to be functioning correctly, you should monitor the passage of packets through the system.
5. Execute the "`fw monitor -v <VSID>`" commands to capture details of packets at multiple points. This may return multiple reports on the same packet as it passes various capture points. This command does not report on Virtual Routers, except for packets destined to an external Virtual Router.

6. Execute the "`tcpdump`" command to display transmitted or received packets for specific interfaces, including Warp interfaces. This often provides valuable clues for resolving connectivity issues.

Troubleshooting Specific Problems

Cannot Establish SIC Trust for VSX Gateway or VSX Cluster Member

When creating a VSX Gateway or VSX Cluster Member, you cannot establish the SIC trust. SmartConsole shows an error message:

```
Certificate cannot be pushed. Connection error with wait agent.
```

Possible Causes	How to Resolve
Check that you have network connectivity between the VSX Gateway and Management Server by pinging from the VSX system (a ping from the Management Server to the VSX Gateway will not work because of the default security policy installed on the VSX Gateway / VSX Cluster Member). **Make sure the context is `vrf 0` first**.	On all applicable machines, re-check the cables, routes, IP addresses and any intermediate networking devices (routers, switches, hubs, and so on) between the Management Server and the VSX Gateway.
Check that all the Check Point processes on the VSX Gateway (s) are up and running by running `cpwd_admin list` and making sure each line has a non-zero value in the `PID` field.	If the VSX Gateway just rebooted, the Check Point processes might still be coming up.
Check that the CPD process is listening to the trust establishment port.	Run the "`netstat -an | grep 18211`" command on the VSX Gateway, and make sure that output looks like this: `tcp 0 0 0.0.0.0:18211 0.0.0.0:* LISTEN`

SIC Trust Problems with New Virtual Devices

When creating a new Virtual System, Virtual Router or Virtual Switch, you cannot establish the SIC trust.

Possible Causes	How to Resolve
Time or time zone mismatch between the Management Server and the VSX Gateway. For proper SIC operation, the time, date and time zone must be synchronized between the Management Server and Gateways/ VSX Cluster Members. Execute the "`/bin/date -u`" command on all machines, to obtain the correct UTC/GMT time. The machines can be in different time zones, as long as their UTC/GMT times match.	Change the time, date and time zone on the Management Server and/or the VSX Gateway, so that their UTC/GMT times match. Refer to your operating system documentation for the exact commands needed to accomplish this.

Install Policy Error Using VSX Creation Wizard

After completing the VSX creation wizard, a failure occurs and the following message appears in the **Operation Report** window:

```
Error: Default policy installation failed on VSX. Install policy
manually using SmartConsole.
```

Possible Causes	How to Resolve
Missing or invalid license on the Management Server. Execute `cplic check` on the Management Server to make sure that you have the required licenses.	Obtain and install the appropriate licenses.
Missing or invalid VSX Gateway / VSX Cluster licenses. Run the "`vsx stat`" command on the VSX Gateway, and make sure that the number is greater than 0 (zero) in the output: `Number of Virtual Systems allowed by license:`	Obtain a VSX and install a valid license for each VSX Gateway / VSX Cluster Members.
Time or time zone mismatch between the Management Server and the VSX Gateway. For proper SIC operation, the time, date and time zone must be synchronized between the Management Server and the VSX Gateway / VSX Cluster Members. Execute the `/bin/date -u` command on all machines, to obtain the correct UTC/GMT time. The machines can be in different time zones, as long as their UTC/GMT offsets match.	Change the time, date and time zone on the Management Server and/or the VSX Gateway / VSX Cluster Members, so that their UTC/GMT offsets match. Refer to your operating system documentation for the exact commands needed to accomplish this.

Internal Host Cannot Ping Virtual System

After defining a Virtual System with an internal VLAN interface, an internal host on that VLAN cannot ping the Virtual System internal or external IP address.

Possible Causes	How to Resolve
A policy allowing the communication was not installed on the Virtual System. Note that after creating a Virtual System, it has a Default Policy that blocks all traffic.	Install a policy on the Virtual System that enables the traffic. In SmartConsole **Logs & Events** view, analyze the logs to make sure that the Virtual System allows the traffic.
There is the VLAN configuration problem on a switch, or physical cable problem.	Check the switch configuration. Make sure that VLAN tag configured on the switch is the same as used for the Virtual System VLAN interface. Check the cables, and make sure that you have plugged the cable from the switch to the correct port on the VSX Gateway / VSX Cluster Members.
Incorrect routing on adjacent routers or hosts.	Check the routing tables on intermediate routers and hosts. You can use the `tcpdump` command on the applicable VLAN interface on the VSX Gateway / VSX Cluster Members to make sure that the traffic arrives to and leaves the VSX Gateway / VSX Cluster Members.
Incorrect IP address or net mask defined on the Virtual System VLAN interface.	Check the IP address and the net mask assigned to the Virtual System internal VLAN interface.

Re-establishing the SIC Trust with Virtual Devices

In the event you encounter connectivity problems due to the loss of the SIC Trust for a specific Virtual Device (Virtual System or Virtual Router), you can use the procedure below to manually re-establish the SIC trust.

To manually re-establish the SIC Trust with a Virtual Device:

Follow the instructions in the sk34098.

1. On the VSX Gateway or each VSX Cluster Member:
   a. Connect to the command line the VSX Gateway or each VSX Cluster Member.
   b. Log in to the Expert mode.
   c. Examine the VSX configuration to determine the ID of the Virtual Device:

      ```
      vsx stat -v
      ```

   d. Reset the SIC with the specified Virtual Device:

      ```
      vsx sic reset <VSID>
      ```

2. On the Management Server:
   a. Connect to the command line the Management Server.
   b. Log in to the Expert mode.
   c. On the Multi-Domain Server, change the context to the applicable Target Domain Management Server that manages the Virtual Device:

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

   d. Determine the SIC name of the Virtual Device:

      ```
      cpca_client lscert -stat valid -kind SIC | grep -i -A 2
      <Name of Virtual Device Object>
      ```

   e. Revoke the SIC certificate of the Virtual Device:

      ```
      cpca_client revoke_cert -n <CN=...,O=...,>
      ```

3. Connect with SmartConsole to the Security Management Server or Main Domain Management Server that manages the VSX Cluster.
4. From the **Gateways & Servers** view or **Object Explorer**, double-click the Virtual Device object.

5. Click **OK**.

   This action creates a new SIC certificate for the Virtual Device and saves it on the VSX Gateway or each VSX Cluster Member.

Command Line Reference

See the *R82 CLI Reference Guide*.

Below is a limited list of applicable commands.

Syntax Legend for CLI Commands

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

Character	Description

TAB	Shows the available nested subcommands:
	`main command`
	`→ nested subcommand 1`
	`→ → nested subsubcommand 1-1`
	`→ → nested subsubcommand 1-2`
	`→ nested subcommand 2`
	Example:
	`cpwd_admin`
	`config`
	`-a <options>`
	`-d <options>`
	`-p`
	`-r`
	`del <options>`
	Meaning, you can run only **one** of these commands:
	■ This command: `cpwd_admin config -a <options>`
	■ Or this command: `cpwd_admin config -d <options>`
	■ Or this command: `cpwd_admin config -p`
	■ Or this command: `cpwd_admin config -r`
	■ Or this command: `cpwd_admin del <options>`

Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.

Character	Description
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

cpconfig

Description

This command starts the Check Point Configuration Tool.

This tool configures specific settings for the installed Check Point products.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must connect to the applicable Security Group.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpconfig
```

Syntax on a Scalable Platform Security Group in Gaia gClish or the Expert mode

```
cpconfig
```

Menu Options

Note - The options shown depend on the configuration and installed products.

Menu Option	Description
Licenses and contracts	Manages Check Point licenses and contracts on this Security Gateway or Cluster Member.
SNMP Extension	Obsolete. Do **not** use this option anymore. To configure SNMP, see the *R82 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.
PKCS#11 Token	Register a cryptographic token, for use by Gaia Operating System. See details of the token, and test its functionality.
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.

Menu Option	Description
Secure Internal Communication	Manages SIC on the Security Gateway or Cluster Member. This change requires a restart of Check Point services on the Security Gateway or Cluster Member. For more information, see: ■ The *R82 Security Management Administration Guide*. ■ sk65764: How to reset SIC.
Enable cluster membership for this gateway	Enables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the: ■ *R82 Installation and Upgrade Guide*. ■ *R82 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (ElasticXL, Maestro, and Chassis).
Disable cluster membership for this gateway	Disables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the: ■ *R82 Installation and Upgrade Guide*. ■ *R82 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (ElasticXL, Maestro, and Chassis).
Enable Check Point Per Virtual System State	Enables Virtual System Load Sharing on the VSX Cluster Member. For more information, see *"Configuring Virtual System Load Sharing (VSLS)" on page 213*. **Note** - This section does **not** apply to Scalable Platforms (ElasticXL, Maestro, and Chassis).
Disable Check Point Per Virtual System State	Disables Virtual System Load Sharing on the VSX Cluster Member. For more information, see *"Configuring Virtual System Load Sharing (VSLS)" on page 213*. **Note** - This section does **not** apply to Scalable Platforms (ElasticXL, Maestro, and Chassis).

Menu Option	Description
Enable Check Point ClusterXL for Bridge Active/Standby	Enables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the: ■ *R82 Installation and Upgrade Guide*. ■ *R82 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (ElasticXL, Maestro, and Chassis).
Disable Check Point ClusterXL for Bridge Active/Standby	Disables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the: ■ *R82 Installation and Upgrade Guide*. ■ *R82 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (ElasticXL, Maestro, and Chassis).
Check Point CoreXL	Manages CoreXL and Firewall mode on the Security Gateway / Cluster Member / Scalable Platform Security Group. After all changes in CoreXL configuration, you must reboot the Security Gateway / Cluster Member / Security Group. For more information, see the *R82 Performance Tuning Administration Guide*.
Automatic start of Check Point Products	Shows and controls which of the installed Check Point products start automatically during boot.
Exit	Exits from the Check Point Configuration Tool.

Example 1 - Menu on a single Security Gateway

```
[Expert@MySingleGW:0]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) SNMP Extension
(3) PKCS#11 Token
(4) Random Pool
(5) Secure Internal Communication
(6) Enable cluster membership for this gateway
(7) Check Point CoreXL
(8) Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :
```

Example 2 - Menu on a Cluster Member

```
[Expert@MyClusterMember:0]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) SNMP Extension
(3) PKCS#11 Token
(4) Random Pool
(5) Secure Internal Communication
(6) Disable cluster membership for this gateway
(7) Enable Check Point Per Virtual System State
(8) Enable Check Point ClusterXL for Bridge Active/Standby
(9) Check Point CoreXL
(10) Automatic start of Check Point Products

(11) Exit

Enter your choice (1-11) :
```

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 a Security Gateway / ClusterXL / Scalable Platform Security Group).

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

On a Security Gateway / ClusterXL / Scalable Platform 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.

vsenv

Description

Changes the shell's current context to the specified Virtual Device.

Syntax

```
vsenv [{<VSID> | <Name of Virtual Device>}]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
No Parameters	Changes the context to the default Virtual Device 0.
<VSID>	Specifies the Virtual Device by its ID.
<Name of Virtual Device>	Specifies the Virtual Device by its Name.

Note - To see the configured Virtual Devices, run the "`vsx stat -v`" command.

Example 1 - Changing the context to the default Virtual Device 0

```
[Expert@MyVsxGW:0]# vsenv
Context is set to Virtual Device VSX2_192.168.3.242 (ID 0).
[Expert@MyVsxGW:0]#
```

Example 2 - Changing the context to the specific Virtual Device

```
[Expert@MyVsxGW:0]# vsenv 2
Context is set to Virtual Device VS2 (ID 2).
[Expert@MyVsxGW:2]#
```

VSX

Description

- Shows VSX configuration.
- Fetches VSX configuration.
- Shows and configures Memory Resource Control.

Syntax

```
vsx
      fetch <options>
      fetch_all_cluster_policies
      fetchvs <options>
      get
      mstat <options>
      resctrl
      showncs <options>
      sicreset
      stat <options>
      unloadall
      vspurge
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Note - The `fw6 vsx` commands are **not** supported.

Parameters

Parameter	Description
`fetch <options>`	Fetches configuration for VSX Gateway. See *"vsx fetch" on page 306*.
`fetch_all_cluster_policies`	Fetches security policy for all Virtual Systems and Virtual Routers from cluster peers. See *"vsx fetch_all_cluster_policies" on page 308*.
`fetchvs <options>`	Fetches configuration for a Virtual System. See *"vsx fetchvs" on page 309*.

Parameter	Description
`get`	Shows the information about the current VSX context. See *"vsx get" on page 310*.
`mstat <options>`	Shows and configures Memory Resource Control. See *"vsx mstat" on page 311*.

Parameter	Description

`resctrl`	From R80.40, the CPU Resource Control is integrated into the CPView utility.
	1. Go to the context of Virtual System 0:
	■ In the Expert mode:
	`vsenv`
	■ In Gaia Clish:
	`set virtual-system 0`
	2. Run the CPView:
	`cpview`
	See *"cpview" on page 299*.
	3. From the top, click:
	Advanced > VSX > VSs > Physical-Resources
	Notes:
	■ This tab shows the CPU consumption by Virtual Systems and by Virtual Routers.
	■ The "**CPU %**" column shows the percentage of CPU used by all the processes of each Virtual System.
	The column shows a percentage of a single CPU (the same behavior as in the "`top`" command).
	Example:
	• There are 4 CPU cores on the VSX Gateway.
	• The processes of the Virtual System "VS1" are using:
	◦ 30% of CPU 0
	◦ 40% of CPU 1
	◦ 50% of CPU 2
	◦ 10% of CPU 3
	In such case, the "**CPU %**" column shows 130% for VS1.
	■ To get the CPU usage for the VSX Gateway / VSX Cluster Member, divide the "**CPU %**" value in the **Total Resource Consumption** section by the number of the CPU cores.

`showncs <options>`	Shows Check Point Network Configuration Script (NCS) for Virtual Device. See *"vsx showncs" on page 315*.

Parameter	Description
`sicreset`	Resets SIC for Virtual System or Virtual Router in the current VSX context. See *"vsx sicreset" on page 316*.
`stat <options>`	Shows status information for VSX Gateway. See *"vsx stat" on page 317*.
`unloadall`	Unloads security policy for all Virtual Systems and Virtual Routers. See *"vsx unloadall" on page 320*.
`vspurge`	Cleans unused entries for Virtual Devices. Fetches configuration file for Virtual Devices. See *"vsx vspurge" on page 321*.

vsx fetch

Description

Fetches the most current configuration files from the Security Management Server or Main Domain Management Server, and applies it to the VSX Gateway.

Syntax

```
vsx fetch [-v] [-q] [-s] local
vsx fetch [-v | -q | -s] [-f <Configuration File>]
vsx fetch [-v | -q] -C "NCS Command"
vsx fetch [-v | -q | -c | -n | -s] [<Management Server>]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-c`	Specifies that this is a VSX Cluster.
`-n`	Specifies not to apply the `local.vsall`, if VSX configuration, as fetched from Management Server, is up-to-date.
`-q`	Specifies to run in quiet mode - shows only summary information.
`-s`	Specifies to fetch concurrently for multi-processor environment.
`-v`	Specifies to run in verbose mode - shows detailed information.
`local`	Reads the configuration file `$FWDIR/state/local/VSX/local.vsall` and executes the Network Configuration Script (NCS).
`-f <Configuration File>`	Fetches the specified configuration with NCS commands file instead of the default `local.vsall` file.
`-C "NCS Command"`	Executes the specified NCS command.

Parameter	Description
<Management Server>	Fetches the `local.vsall` from the specified Management Server (by resolvable hostname, or IP address), replaces and runs it. **Note** - If you do not specify the Management Server explicitly, the command takes it from the `$FWDIR/conf/masters` file on the VSX Gateway.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example

```
[Expert@MyVsxGW:0]# vsx fetch
Fetching VSX Configuration From: 192.168.30.40

 Local VSX Configuration is Up-To-Date.
 Cleaning un-used Virtual Systems entries (local.vskeep).

 Purge operation succeeded.
 Fetching Virtual Systems configuration file (local.vsall).

SecureXL device has been enabled for vsid 1
SecureXL device has been enabled for vsid 2
SecureXL device has been enabled for vsid 3
Virtual Systems configuration file installed successfully
[Expert@MyVsxGW:0]#
```

vsx fetch_all_cluster_policies

Description

Fetches security policy for all Virtual Systems and Virtual Routers from cluster peers.

Syntax

```
vsx fetch_all_cluster_policies [-v]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-v`	Specifies to run in verbose mode - shows detailed information.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx fetchvs

Description

Fetches configuration file for the specified Virtual Device based on information stored locally on the VSX Gateway.

Syntax

```
vsx fetchvs [-v | -q] [{<VSID> | <Name of Virtual Device>}]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-q`	Specifies to run in quiet mode - shows only summary information.
`-v`	Specifies to run in verbose mode - shows detailed information.
<Name of Virtual Device>	Specifies the name of the Virtual Device.
<VSID>	Specifies the ID of the Virtual Device.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example

```
[Expert@MyVsxGW:0]# vsx fetchvs 2
```

vsx get

Description

Shows the information about the current VSX context.

Syntax

```
vsx get
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example

```
[Expert@MyVsxGW:0]# vsx get
Current context is VSX Gateway MyVsxGW (ID 2).
[Expert@MyVsxGW:0]#
```

vsx mstat

Description

Shows and configures Memory Resource Control.

Output shows these global memory resources:

Resource	Description
Memory Total	Total physical memory on the VSX Gateway.
Memory Free	Available physical memory.
Swap Total	Total of swap memory.
Swap Free	Available swap memory.
Swap-in rate	Total memory swaps per second.

In addition:

1. Run the `cpview` command (see *"cpview" on page 299*).
2. From the top, click:

   Advanced > VSX > VSs > Physical-Resources

Syntax

```
vsx mstat help
```

```
vsx mstat
      [-vs <VSID>] [unit <Unit>] [sort {<Number> | all}]
      debug
      disable
      enable
      status
      swap <Minutes>
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`help`	Shows the built-in usage.

Parameter	Description
No Parameters	Shows the total memory consumption for each Virtual System.
`-vs <VSID>`	Specifies the Virtual Systems by their IDs. You can specify: ■ One Virtual System. Example: `-vs 1` ■ Many individual Virtual Systems (separate their IDs with spaces). Example: `-vs 2 3` ■ A range of Virtual Systems. Example: `-vs 4-6` **Note** - You can combine all the available options (separate them with spaces). Example: `-vs 1 4-6`
`unit <Unit>`	Specifies the memory measurement unit shown in the command output: ■ `B` - bytes ■ `K` - kilobytes ■ `M` - megabytes (default) ■ `G` - gigabytes
`sort {<Number> | all}`	Sorts the Virtual Systems in the output by their memory size. Specifies the number of Virtual Systems shown in the command output. Use `all` to show all Virtual Systems. If you do not specify this flag, the Virtual Systems in the output are sorted by their VSID.
`debug`	Shows memory consumption debug information for each Virtual System by fields, which are defined in the configuration file.
`disable`	Disables the Memory Resource Control. **Note** - This change applies immediately and does not require a reboot.
`enable`	Enables the Memory Resource Control. **Note** - This change requires a reboot.
`status`	Shows the current Memory Resource Control status.

Parameter	Description
`swap <Minutes>`	Specifies the swap-in sample rate in minutes. Enter the number of minutes that the system measures memory swaps to determine the swap-in rate. Only integers are valid values. The default swap-in sample rate is `10`. **Notes:** ■ Swap-in sample rate is a system-wide Linux setting. When you change the value for memory monitoring, all the swap-in rates are calculated according to the new value. ■ When you enable the monitoring memory resources feature, the swap-in rate setting is saved. When you disable the feature, the system restores the saved setting.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example 1

```
[Expert@MyVsxGW:0]# vsx mstat unit M sort all

VSX Memory Status
=================
Memory Total: 7753.95 MB
Memory Free: 7168.71 MB
Swap Total: 3992.71 MB
Swap Free: 3992.71 MB
Swap-in rate: 8796093022208.00 MB

 VSID | Memory Consumption
======+====================
    0 | 260.79 MB
    1 | 0.00 MB

[Expert@MyVsxGW:0]#
```

Example 2

```
[Expert@MyVsxGW:0]# vsx mstat -vs 0 unit G

VSX Memory Status
=================
Memory Total: 7.572 GB
Memory Free: 7.001 GB
Swap Total: 3.899 GB
Swap Free: 3.899 GB
Swap-in rate: 8589934592.000 GB

 VSID | Memory Consumption
======+====================
    0 |          0.255 GB

[Expert@MyVsxGW:0]#
```

Example 3

```
[Expert@MyVsxGW:0]# vsx mstat debug

VSX Memory Status
=================
Memory Total: 7940048.00 KB
Memory Free: 7339864.00 KB
Swap Total: 4088532.00 KB
Swap Free: 4088532.00 KB
Swap-in rate: 9007199254740992.00 KB

 VSID | Private_Clean | Private_Dirty | DispatcherGConn | DispatcherHTab |    SecureXL |
DispatcherGConn6 | DispatcherHTab6 | SecureXL6

======+===============+===============+=================+================+=============+=======
===========+=================+===========
    0 |   34456.00 KB |  182104.00 KB |         6.09 KB |        0.00 KB | 51071.91 KB |
 0.00 KB |         0.00 KB |   0.00 KB
    1 |       0.00 KB |       0.00 KB |         0.00 KB |        0.00 KB |     0.00 KB |
 0.00 KB |         0.00 KB |   0.00 KB

Note: To add a field to memory table please uncomment the required field (delete the leading
'#')
      To remove a field from memory table please comment out the required field (add a leading
'#')
      Configuration is done in the file /opt/CPsuite-R82/fw1/conf/memoryinfo.conf

[Expert@MyVsxGW:0]#
```

vsx showncs

Description

Shows Check Point Network Configuration Script (NCS) for a Virtual Device.

Syntax

```
vsx showncs {<VSID> | <Name of Virtual Device>}
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
<Name of Virtual Device>	Specifies the name of the Virtual Device.
<VSID>	Specifies the ID of the Virtual Device.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx sicreset

Description

Resets SIC for Virtual System or Virtual Router in the current VSX context.

Notes:

- This operation is **not** supported for the context of VSX Gateway itself (VS0).
- On the Management Server, run the "`cpca_client revoke_cert`" command to cancel the old certificate.
- In SmartConsole, open the Virtual System object and immediately click **OK**. This action creates a new certificate, and transfers the certificate to the VSX Gateway.

Syntax

```
vsenv {<VSID> | <Name of Virtual Device>}
vsx sicreset {<VSID> | <Name of Virtual Device>}
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
<Name of Virtual Device>	Specifies the name of the Virtual Device.
<VSID>	Specifies the ID of the Virtual Device.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx stat

Description

Shows status information for VSX Gateway.

Syntax

```
vsx stat [-l] [-v] [<VSID>]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-l`	Shows a list of all Virtual Devices and their applicable information.
`-v`	Shows a summary table with all Virtual Devices.
<VSID>	Specifies a Virtual Device by its ID.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example 1 - Show a summary table with all Virtual Devices.

```
[Expert@MyVsxGW:2]# vsx stat -v
VSX Gateway Status
==================
Name:            VSX1_192.168.3.241
Access Control Policy: VSX_Cluster_VSX
Installed at:    20Sep2019 22:06:33
Threat Prevention Policy: <No Policy>
SIC Status:      Trust

Number of Virtual Systems allowed by license:          25
Virtual Systems [active / configured]:                  2 / 2
Virtual Routers and Switches [active / configured]:     0 / 0
Total connections [current / limit]:                    5 / 44700

Virtual Devices Status
======================

 ID  | Type & Name | Access Control Policy | Installed at    | Threat Prevention Policy | SIC
Stat
-----+-------------+-----------------------+-----------------+--------------------------+-------
--
   1 | S VS1       | VS_Policy             | 20Sep2019 22:07 | <No Policy>              | Trust
   2 | S VS2       | VS_Policy             | 20Sep2019 22:07 | <No Policy>              | Trust

Type: S - Virtual System, B - Virtual System in Bridge mode,
      R - Virtual Router, W - Virtual Switch.

[Expert@MyVsxGW:2]#
```

Example 2 - Show a list of all Virtual Devices and their applicable information.

```
[Expert@MyVsxGW:2]# vsx stat -l

VSID:            0
VRID:            0
Type:            VSX Gateway
Name:            VSX1_192.168.3.241
Security Policy: VSX_Cluster_VSX
Installed at:    20Sep2019 22:06:33
SIC Status:      Trust
Connections number: 5
Connections peak:   43
Connections limit:  14900

VSID:            1
VRID:            1
Type:            Virtual System
Name:            VS1
Security Policy: VS_Policy
Installed at:    20Sep2019 22:07:03
SIC Status:      Trust
Connections number: 0
Connections peak:   3
Connections limit:  14900

VSID:            2
VRID:            2
Type:            Virtual System
Name:            VS2
Security Policy: VS_Policy
Installed at:    20Sep2019 22:07:01
SIC Status:      Trust
Connections number: 0
Connections peak:   2
Connections limit:  14900
[Expert@MyVsxGW:2]#
```

Example 3 - Shows the information for the specified Virtual Device

```
[Expert@MyVsxGW:2]# vsx stat 2

VSID:            2
VRID:            2
Type:            Virtual System
Name:            VS2
Security Policy: VS_Policy
Installed at:    20Sep2019 22:07:01
SIC Status:      Trust
Connections number: 0
Connections peak:   2
Connections limit:  14900
[Expert@MyVsxGW:2]#
```

vsx unloadall

Description

Unloads security policy for all Virtual Systems and Virtual Routers.

See sk33065: Unloading policy from a VSX Security Gateway.

Syntax

```
vsx unloadall
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx vspurge

Description

Removes Virtual Devices that are no longer defined in the management database, but were not removed from the VSX Gateway, because the VSX Gateway was down or disconnected when the management server pushed the updated VSX configuration.

This command cleans all unused Virtual Devices entries (from the NCS `local.vskeep`) and fetches the VSX configuration file (NCS `local.vskeep`) again.

Syntax

```
vsx vspurge [-q | -v] [-f <purge_file>]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-q`	Specifies to run in quiet mode - shows only summary information.
`-v`	Specifies to run in verbose mode - shows detailed information.
`-f <purge_file>`	Specifies the path and the name of the file, in which the command saves the purged information.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx_util

Description

Performs various VSX maintenance tasks.

You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main* Domain Management Server on Multi-Domain Server).

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util -h
```

```
vsx_util <Command> [-s <Mgmt Server>] [-u <UserName>] [-c <Name of VSX Object>] [-m <Name of VSX Cluster Member>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
<Command>	Specifies the `vsx_util` sub-command. See the table below.
`-s` *<Mgmt Server>*	Specifies the IP address or resolvable hostname of the Security Management Server, or Main Domain Management Server.
`-u` *<UserName>*	Specifies the administrator username.
`-c` *<Name of VSX Object>*	Specifies the name of the VSX Gateway or VSX Cluster object.
`-m` *<Name of VSX Cluster Member>*	Specifies the name of the VSX Gateway or VSX Cluster Member object.

Important - The `vsx_util` command requires you to enter this information:

- IP address or Hostname of the Security Management Server, or *Main* Domain Management Server.
- Management Server Administrator user name and password.
- The applicable VSX object, on which the command operates.
- Most of the `vsx_util` sub-commands are interactive and require additional user input.

The 'vsx_util' sub-commands

Sub-command	Description
`vsx_util add_member`	Adds a new Cluster Member to a VSX Cluster and pushes the VSX Cluster configuration to the new VSX Cluster Member. See *"vsx_util add_member" on page 327*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util change_ interfaces`	Automatically replaces designated existing interfaces with new interfaces on all Virtual Devices, to which the existing interfaces connect. See *"vsx_util change_interfaces" on page 329*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util change_mgmt_ ip`	Changes the VSX Management IP address (within the same subnet) of a VSX Gateway or VSX Cluster Member. See *"vsx_util change_mgmt_ip" on page 333*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util change_mgmt_ subnet`	Changes (or adds) the VSX Management IP address of a VSX Gateway or VSX Cluster Member to a new subnet. See *"vsx_util change_mgmt_subnet" on page 334*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util change_ private_net`	Changes the IP address of the Internal Communication Network in a VSX Cluster. See *"vsx_util change_private_net" on page 336*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util convert_ cluster`	Converts the VSX Cluster mode between High Availability (default) and Virtual System Load Sharing. See *"vsx_util convert_cluster" on page 338*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).

Sub-command	Description
`vsx_util downgrade`	Downgrades the version of a VSX Gateway or VSX Cluster in the management database. See *"vsx_util downgrade" on page 340*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util reconfigure`	Restores VSX configuration on a VSX Gateway or VSX Cluster Member. See *"vsx_util reconfigure" on page 341*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util remove_ member`	Removes a Cluster Member from a VSX Cluster. See *"vsx_util remove_member" on page 347*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util show_ interfaces`	Shows configuration of selected interfaces - interface types, connections to Virtual Devices, and IP addresses. See *"vsx_util show_interfaces" on page 348*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util upgrade`	Upgrades the version of a VSX Gateway or VSX Cluster in the management database. See *"vsx_util upgrade" on page 352*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util view_vs_conf`	Shows configuration of a Virtual Device on the Management Server versus the VSX Gateway or VSX Cluster. See *"vsx_util view_vs_conf" on page 353*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).

Sub-command	Description
`vsx_util vsls`	Shows the configuration menu for Virtual System Load Sharing - see status, redistribute, export and import configuration. See *"vsx_util vsls" on page 357*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).

Notes

- This command writes its messages to the `vsx_util_YYYYMMDD_HH_MM.log` file on the Management Server:
  - On a Security Management Server:

    ```
    $FWDIR/log/vsx_util_YYYYMMDD_HH_MM.log
    ```

  - On a Multi-Domain Server - if executed the command in the MDS context:

    ```
    /opt/CPsuite-R82/fw1/log/vsx_util_YYYYMMDD_HH_MM.log
    ```

  - On a Multi-Domain Server - if executed the command in the context of a Domain Management Server:

    ```
    /opt/CPmds-R82/customers/<Name of Domain Management Server>/CPsuite-R82/fw1/log/vsx_util_YYYYMMDD_HH_MM.log
    ```

- If it is necessary to exit from the `vsx_util` command's menu, press the **CTRL C** keys.

  Important - Do **not** press these keys, it this command already started to perform a change. If you press these keys during the operation, the command does not save its log file.

vsx_util add_member

Description

Adds a new Cluster Member to a VSX Cluster and pushes the VSX Cluster configuration to the new VSX Cluster Member.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util add_member
```

Required Input

- The applicable VSX Cluster object.
- Name of the new VSX Cluster Member.
- IP address for the management interface.
- IP address for the synchronization interface.
- The one-time Activation Key (SIC activation key)

Comments

- Execute the command and follow the instructions on the screen.
- After the command adds a new Cluster Member to the management database, the command prompts you to reconfigure the new VSX Cluster Member (to push the VSX Cluster configuration to it).
  - If you enter "**y**" to reconfigure the new VSX Cluster Member at this time, then the *"vsx_util reconfigure" on page 341* operation starts automatically on the new VSX Cluster Member.

    Important - You must reboot the new VSX Cluster Member after the reconfigure operation finishes.
  - If you enter "**n**" to cancel the reconfigure operation on the new VSX Cluster Member at this time, then later you must manually run the *"vsx_util reconfigure" on page 341* command for the new VSX Cluster Member.

vsx_util change_interfaces

Description

Automatically replaces designated existing interfaces with new interfaces on all Virtual Devices, to which the existing interfaces connect.

This command is useful when converting a deployment to use Link Aggregation, especially where VLANs connect to many Virtual Devices.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util change_interfaces
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- Where to apply the change (Management Server only, or Management Server and VSX Gateway / VSX Cluster Members).
- Name of the interface to be replaced.
- Name of the new (replacement) interface.

Comments

- Execute the command and follow the instructions on the screen.
- This command supports the resume feature.
- You can use this command to migrate a VSX deployment from an Open Server to a Check Point appliance by using the **Management Only** mode.
- Refer to the **Notes** section below for additional information.

Procedure

Step	Instructions
1	Close all SmartConsole clients that are connected to the Security Management Server or Domain Management Servers.
2	Connect to the command line on the Management Server.
3	Log in to the Expert mode.
4	On Multi-Domain Server, go to the context of the *Main* Domain Management Server that manages the applicable VSX Gateway (VSX Cluster) object: `mdsenv <IP address or Name of Domain Management Server>`
5	Run: `vsx_util change_interfaces`
6	Enter the IP address of the Security Management Server or Main Domain Management Server.
7	Enter the Management Server administrator username and password.
8	Select the VSX Gateway (VSX Cluster) object.
9	When prompted, select one of the following options: ■ **Apply changes to the management database and to the VSX Gateway/Cluster members immediately** Changes the interface on the Management Server and on the VSX Gateway (each VSX Cluster Member). ■ **Apply changes to the management database only** Changes the interface on the Management Server only. You must run the *"vsx_util reconfigure" on page 341* command to push the updated VSX configuration to VSX Gateways (each VSX Cluster Member).
10	Select the interface to be replaced.

Step	Instructions
11	Select the new (replacement) interface. a. You can optionally add a new interface, if you select the **A new interface name** option. This interface must physically exist on the VSX Gateway (all VSX Cluster Members). Otherwise, the operation fails. b. At the prompt, enter the new interface name. If the new interface is a Bond interface, the interface name must match the name of the configured Bond interface exactly.
12	The command prompts you: `Would you like to change another interface? (y|n) [n]:` ■ To replace additional interfaces, enter **y**. ■ To complete the process, enter **n**.
13	If you selected the option **Apply changes to the management database only**, you can remove the old (replaced) interfaces from the management database. When prompted, enter **y**: `Would you like to remove the old interfaces from the database? (y|n) [n]: y`
14	Reboot the VSX Gateway (all VSX Cluster Members).

Notes

- The option "**Apply changes to the management database and to the VSX Gateway/Cluster members immediately**" verifies connectivity between the Management Server and the VSX Gateway or VSX Cluster Members. In the event of a connectivity failure one of the following actions occur:

  1. If **all** of the newly changed interfaces fail to establish connectivity, the process terminates unsuccessfully.
  2. If one or more interfaces successfully establish connectivity, while one or more other interfaces fail, you may optionally continue the process.

     In this case, those interfaces for which connectivity was established successfully will be changed.

     For those interfaces that failed, you must then resolve the issue and then run the *"vsx_util reconfigure" on page 341* command to complete the process.

- If you select the option "**Apply changes to the management database only**", you can select one of these:

  - Another interface from list (if any are available).
  - Option to add a new interface.

vsx_util change_mgmt_ip

Description

Changes the VSX Management IP address of a VSX Gateway or VSX Cluster Member.

This command changes the Management IP address within the same subnet.

For more information, see sk92425.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util change_mgmt_ip
```

Required Input

- The applicable VSX Cluster object.
- The applicable VSX Cluster Member object.
- New management IP address.

Comments

- Execute the command and follow the instructions on the screen.

vsx_util change_mgmt_subnet

Description

Changes the VSX Management IP address of a VSX Gateway or VSX Cluster Member.

This command changes the Management IP address from the current subnet to a different subnet.

For more information, see sk92425.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util change_mgmt_subnet
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- New management IPv4 address.
- New management IPv4 netmask.
- New management IPv6 address.
- New management IPv6 prefix.
- New IPv4 default gateway.
- New IPv6 default gateway.

Comments

- Execute the command and follow the instructions on the screen.
- This command updated only routes that were automatically generate.

  You must remove and/or change all manually created routes that use the previous management subnet.
- You must reboot the VSX Gateway (all VSX Cluster Members) after the command finishes.

vsx_util change_private_net

Description

Changes the IP address of the Internal Communication Network in a VSX Cluster (cluster private network).

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util change_private_net
```

Required Input

- The applicable VSX Cluster object.
- New IPv4 address for the cluster private network.
- New IPv4 netmask for the cluster private network.
- New IPv6 address and prefix for the cluster private network.

Comments

- Run the command and follow the instructions on the screen.
- The IP address of the Internal Communication Network must be unique.

  This IP address must **not** be used anywhere in your environment, including the Virtual Devices on this VSX Cluster.
- The illegal IPv4 addresses are: `0.0.0.0`, `127.0.0.0`, and `255.255.255.255`
- For IPv4 address, the network mask must be one of these:
  - `255.255.0.0`, or `/16`
  - `255.255.128.0`, or `/17`
  - `255.255.192.0`, or `/18`
  - `255.255.224.0`, or `/19`
  - `255.255.240.0`, or `/20`
  - `255.255.248.0`, or `/21`
  - `255.255.252.0`, or `/22` (this is the default)
- For IPv6 address, the new prefix must be `/80`.

vsx_util convert_cluster

Description

Converts the VSX Cluster mode between High Availability (default) and Virtual System Load Sharing.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Important:

- The only mode available for a VSX Cluster that was installed as R81.10 and higher is **Virtual System Load Sharing (VSLS)**.
- The **High Availability** mode is available only if you upgrade a VSX Cluster from R81 or lower to R82.
  You can also convert a VSLS cluster to the High Availability mode (see *"Changing the VSX Cluster Type" on page 208*).
- It is not supported to run the `vsx_util convert_cluster` command to convert a VSX Cluster from the High Availability mode to the VSLS mode when the VSX Cluster contains a Virtual Switch that is not assigned to any physical interface or to a VLAN interface.

Syntax

```
vsx_util convert_cluster
```

Required Input

- The applicable VSX Cluster object.
- The ClusterXL mode (case sensitive).

Comments

- Execute the command and follow the instructions on the screen.
- When you convert from Virtual System Load Sharing to High Availability:

- All Virtual Systems are **Active** on the same VSX Cluster Member by default.
- Peer Virtual Systems are **Standby** on other VSX Cluster Members.

vsx_util downgrade

Description

Downgrades the version of a VSX Gateway or VSX Cluster in the management database.

Important - You can use this command only if you did **not** make any configuration changes after you used the "`vsx_util upgrade`" command.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util downgrade
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- The applicable Check Point version.

Comments

- Used only to revert the upgraded VSX Gateway or VSX Cluster object.
- Execute the command and follow the instructions on the screen.
- To deploy the version change to the VSX Cluster Members, you must run the *"vsx_util reconfigure" on page 341* command.

vsx_util reconfigure

Description

Restores VSX configuration on a VSX Gateway or VSX Cluster Member (for example, after you perform clean install after a system failure).

Syntax

```
vsx_util reconfigure
```

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Important - Before you run this command on the Management Server, you must configure specific settings on the cleanly installed VSX Gateway or VSX Cluster Member as they were:

- IP address of Gaia management interface
- Enable IPv6 support in Gaia
- Configure the applicable interfaces (Bond, VLAN, and so on)
- Configure kernel parameters and their values:
  - `$FWDIR/boot/modules/fwkern.conf`
  - `$PPKDIR/conf/simkern.conf`
- Configure CoreXL:
  - Number of CoreXL Firewall instances (for IPv4 and IPv6) in the context of VS0 (run the `cpconfig` command and select the option **Check Point CoreXL**)
  - `$FWDIR/conf/fwaffinity.conf`

Important - While the "`vsx_util reconfigure`" command is running on the Management Server, it is not supported to make any configuration changes on the Scalable Platform Security Group. You must wait until all Security Group Members and Virtual Systems are up and running (Limitation ID 01812597).

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- The one-time Activation Key (SIC activation key).

Comments

- Execute the command and follow the instructions on the screen.
- The new VSX Gateway or VSX Cluster Member:
  - Must be a *new* installation.

    You cannot use a VSX Gateway or VSX Cluster Member with a previous VSX configuration.
  - Must have the same hardware specifications as the original.

    Most importantly, it must have *at least* the same number of interfaces.
  - Must have the same Gaia OS configuration as the original.

    Most importantly, it must have the same VSX Management IP address.

Limitations

The reconfigure process does **not** restore the local configuration that was performed on VSX Gateway or VSX Cluster Member itself (because this configuration is not stored on the Management Server).

Important - After the reconfigure process is complete and you rebooted VSX Gateway or VSX Cluster Member, you must manually configure these settings from scratch or from backed up files.

These settings and files are **not** restored during the reconfigure process and you must manually configure them again:

- Per Virtual System State - run the "`cpconfig`" command and examine the option "`Per Virtual System State`". The title of this option must be the same on each VSX Cluster Member - either "`Enable Check Point Per Virtual System State`" or "`Disable Check Point Per Virtual System State`". To change this configuration, enter the number of this option and follow the instructions on the screen.

  Note - Do not change the value of the kernel parameter "`fwha_enable_state_machine_by_vs`" in the `$FWDIR/boot/modules/fwkern.conf` file. The VSX Cluster changes this value automatically.

- Any OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).
- Backup files and Gaia snapshots saved in the past on the VSX Gateway or VSX Cluster Member.
- Any settings manually defined in various configuration files on the VSX Gateway or VSX Cluster Member.
- Any Check Point configuration files.

  Note - Some of these files do not exist by default. Some files are configured on each VSX Gateway and VSX Cluster Member, and some files are configured for each Virtual System.

  List of the most important files

  Note - Some of these files do not exist by default. Some files are configured on each VSX Gateway and VSX Cluster Member, and some files are configured in the context of each Virtual System.

  This list is sorted alphabetically.

  - `$CVPNDIR/conf/cvpnd.C`
  - `$FWDIR/boot/modules/fwkern.conf`
  - `$FWDIR/conf/cpha_bond_ls_config.conf`

- `$FWDIR/conf/cpha_specific_vlan_data.conf` (see sk92784)
- `$FWDIR/conf/discntd.if`
- `$FWDIR/conf/fw_fast_accel_export_configuration.conf` (see sk156672)
- `$FWDIR/conf/fwaffinity.conf`
- `$FWDIR/conf/fwauthd.conf`
- `$FWDIR/conf/hsm_configuration.C`
- `$FWDIR/conf/identity_broker.C`
- `$FWDIR/conf/ipassignment.conf`
- `$FWDIR/conf/local.arp` (see sk30197)
- `$FWDIR/conf/malware_config`
- `$FWDIR/conf/prioq.conf` (see sk105762)
- `$FWDIR/conf/rad_conf.C`
- `$FWDIR/conf/synatk.conf`
- `$FWDIR/conf/te.conf`
- `$FWDIR/conf/thresholds.conf`
- `$FWDIR/conf/trac_client_1.ttm`
- `$FWDIR/conf/vsaffinity_exception.conf`
- `$PPKDIR/conf/simkern.conf`
- `/var/ace/sdconf.rec`
- `/var/ace/sdopts.rec`
- `/var/ace/sdstatus.12`
- `/var/ace/securid`

Example

This example shows how the VSX configuration is restored on a VSX Cluster Member.

```
[Expert@MDS:0]# vsx_util reconfigure

************************************************************************************
* Note: the operation you are about to perform changes the information in the management *
* database. Back up the database before continuing.                                  *
************************************************************************************

Enter Security Management Server/main Domain Management Server IP address (Hit 'ENTER' for
'localhost'): 192.168.3.240
Enter Administrator Name: ******
Enter Administrator Password: ******
Select VSX gateway/cluster object name:
  1)    VSX_Cluster
Select: 1


Select VSX member name to reconfigure:
  1)    VSX1_192.168.3.241
  2)    VSX2_192.168.3.242
Select: 1
You are about to perform reconfigure on VSX gateway/cluster, please read sk97552.
Are you sure you want to continue [y/n]? y
Enter Activation Key:
Retype Activation Key:


 1/10 : Certificate Revocation              [########################################] 100%
00:00:01
 2/10 : Certificate Replacement             [########################################] 100%
00:00:06
 3/10 : Connectivity Check                  [########################################] 100%
00:00:05
 4/10 : Fetching Configuration              [########################################] 100%
00:00:02
 5/10 : Verifying Configuration             [########################################] 100%
00:00:00
 6/10 : Installing policy on: VSX_Cluster   [########################################] 100%
00:00:21
 7/10 : Converting Gateway to VSX           [########################################] 100%
00:02:13
 8/10 : Generating Activation Keys          [########################################] 100%
00:00:00
 9/10 : Reconfiguring                       [########################################] 100%
00:00:03
10/10 : Pushing Configuration               [########################################] 100%
00:00:44

Database saved successfully.
```

```
==================== SUMMARY ====================
---- Reconfigure gateway operation completed successfully

************************************************************
IMPORTANT:
   When you are managing a VSX cluster,
   make sure that the new reconfigured member has the same number of
   IPv4, and IPv6 firewall instances as the other VSX cluster members.
   Run cpconfig command to show and edit CoreXL settings.
NOTE:
   In case of adding a new cluster member to a VSX Cluster,
   while using 'ClusterXL Virtual System Load Sharing'
   make sure to run 'vsx_util vsls' after rebooting the
   gateway in order for the Virtual Systems to become active
   on the newly added VSX cluster member.

IMPORTANT: Please reboot the gateway

************************************************************

Logging details are available at /opt/CPmds-R82/customers/MyDomain_Server/CPsuite-
R82/fw1/log/vsx_util_20190917_13_16.log

[Expert@MDS:0]#
```

vsx_util remove_member

Description

Removes a Cluster Member from a VSX Cluster.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util remove_member
```

Required Input

- The applicable VSX Cluster object.
- The applicable VSX Cluster Member object.

Comments

- Before you run this command:
  - Make sure to remove (detach) the license from the VSX Cluster Member.
  - Make sure to run the "`cphastop`" command to avoid unexpected failover from the VSX Cluster Member.
  - Make sure to disconnect the VSX Cluster Member from all networks, except from the Management Server.
- Execute the command and follow the instructions on the screen.

vsx_util show_interfaces

Description

Shows configuration of selected interfaces - interface types, connections to Virtual Devices, and IP addresses.

The command shows the information on the screen and also saves it to the `interfacesconfig.csv` file in the current working directory.

Important - On a Multi-Domain Security Management Server, you must switch to the context of the **Main**Domain Management Server that manages the VSX Gateway / VSX Cluster object.
Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util show_interfaces
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- Which interfaces to show:

Menu Option	Description
1) All Interfaces	Shows all interfaces (Physical and Warp).
2) All Physical Interfaces	Shows only Physical interfaces.
3) All Warp Interfaces	Shows only Warp interfaces.
4) A Specific Interface	Prompts you to enter the name of the specific interface to show. **Note** - You cannot specify a VLAN tag as a parameter. You can, however, specify an interface used as a VLAN (without the tag) to see all VLAN tags associated with that interface. See the example below.

Example

```
[Expert@MGMT:0]# vsx_util show_interfaces
Enter Security Management Server/main Domain Management Server IP address (Hit 'ENTER' for
'localhost'): 172.16.16.240
Enter Administrator Name: admin
Enter Administrator Password:

Select VSX gateway/cluster object name:
  1)    VSX_Cluster_1
  2)    VSX_Cluster_2
  3)    VSX_GW_1
  4)    VSX_GW_2
Select: 1

Which interface would you like to display?
  1)    All Interfaces
  2)    All Physical Interfaces
  3)    All Warp Interfaces
  4)    A Specific Interface
Enter your choice: 1

+-------------------+---------------------+----+-----------------------------------------------
--+
| Type & Interface  | Virtual Device Name |VSID| IP / Mask length
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|M eth0             |VSX_Cluster_1        |0   |v4 172.16.16.98/24 v6 2001:0DB8::98/64
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|S eth1             |VSX_Cluster_1        |0   |v4 10.0.0.0/24
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|U eth2             |VS1                  |1   |v4 192.0.2.2/24 v6 2001:0DB8:c::1/64
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|U eth3             |VS1                  |1   |v4 192.168.3.3/24 v6 2001:0DB8:b::1/64
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|A eth4             |                     |    |
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|U eth5             |VS2                  |2   |v4 10.10.10.10/24 v6 2001:0DB8:a::1/64
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|A eth6             |                     |    |
 |
+-------------------+---------------------+----+-----------------------------------------------
--+

#Type: M - Management Interface    S - Synchronization Interface
#      V - VLAN Interface          W - Warp Interface
#      U - Used Interface          A - Available Interface
#      X - Unknown Interface       E - Error in Interface Properties

Logging details are available at /opt/CPsuite-R82/fw1/log/vsx_util_20210625_17_45.log

[Expert@MGMT:0]#
[Expert@MGMT:0]# cat interfacesconfig.csv
 Interface Name , Type ,Virtual Device Name , VSID , IPv4 Address , IPv4 mask length, IPv6 Address,
IPv6 mask length
```

```
eth0,M,VSX_Cluster_1,0,172.16.16.98,24,2001:0DB8::98,64
eth1,S,VSX_Cluster_1,0,10.0.0.0,24,,
eth2,U,VS1,192.0.2.2,24,2001:0DB8:c::1,64
eth3,U,VS1,192.168.3.3,24,2001:0DB8:b::1,64
eth4,A
eth5,U,VS2,10.10.10.10,24,2001:0DB8:a::1,64
eth6,A

#Type: M - Management Interface    S - Synchronization Interface
#      V - VLAN Interface          W - Warp Interface
#      U - Used Interface          A - Available Interface
#      X - Unknown Interface       E - Error in Interface Properties

[Expert@MGMT:0]#
```

vsx_util upgrade

Description

Upgrades the version of a VSX Gateway or VSX Cluster in the management database.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util upgrade
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- The applicable Check Point version.

Comments

- Execute the command and follow the instructions on the screen.
- After the command finishes, you must run the *"vsx_util reconfigure" on page 341* command.
- To revert this upgrade, run the *"vsx_util downgrade" on page 340* command.

vsx_util view_vs_conf

Description

Compares the configuration of all Virtual Devices on the Management Server and the actual configuration on the VSX Gateway or VSX Cluster Members.

Important - On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util view_vs_conf
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- The applicable Virtual Device object.

Example

```
[Expert@MGMT:0]# vsx_util view_vs_conf
Enter Security Management Server/main Domain Management Server IP address (Hit 'ENTER' for
'localhost'): 172.16.16.240
Enter Administrator Name: admin
Enter Administrator Password:

Select VSX gateway/cluster object name:
  1)    VSX_Cluster_1
  2)    VSX_Cluster_2
  3)    VSX_GW
  4)    VSX_GW_2
Select: 1

Select Virtual Device object name:
  1)    VS1
  2)    VS2
  3)    VS3
  4)    VSX_Cluster
Select: 1

Type: Virtual System

Interfaces configuration table:

+-------------------------------------------------+-----+-------------------+
|Interfaces                                       |Mgmt |VSX GW(s)          |
+----------+--------------------------------------+-----+---------+---------+
|Name      |IP / Mask length                      |     |mem 1    |mem2     |
+----------+--------------------------------------+-----+---------+---------+
|eth2      |v4 10.0.0.0/24 v6 2001:db8::abc::1/64   |  V  |    V    |    V    |
|eth3      |v4 10.10.10.10/24 v6 2001:db8::3121/64  |  V  |    V    |    V    |
+----------+--------------------------------------+-----+---------+---------+


Interfaces Table Legend:

  V   - Interface exists on the gateway and matches management information (if defined on the
management).
  -   - Interface does not exist on the gateway.
 N/A  - Fetching Virtual Device configuration from the gateway failed.
 !IP  - Interface exists on the gateway, but there is an IP address mismatch.
!MASK - Interface exists on the gateway, but there is a Net Mask mismatch.


Routing table:

+-----------------------------------------------------------+-----+-------------+
|Ipv4 Routes                                                |Mgmt |VSX GW(s)    |
+--------------------------+--------------------+-----------+-----+------+------+
|Destination / Mask Length |Gateway             |Interface  |     |mem1  |mem2  |
+--------------------------+--------------------+-----------+-----+------+------+
|2.2.2.0/24                |                    |eth2       |  V  |  V   |  V   |
|3.3.3.0/24                |                    |eth3       |  V  |  V   |  V   |
+--------------------------+--------------------+-----------+-----+------+------+
+--------------------------+--------------------+-----------+-----+------+------+


+-----------------------------------------------------------+-----+-------------+
|Ipv6 Routes                                                |Mgmt |VSX GW(s)    |
+--------------------------+--------------------+-----------+-----+------+------+
|Destination / Mask Length |Gateway             |Interface  |     |mem1  |mem2  |
+--------------------------+--------------------+-----------+-----+------+------+
|2001:db8::abc::/64        |                    |eth2       |  V  | !NH  | !NH  |
|2001:db8:0a::/64          |                    |eth3       |  V  | !NH  | !NH  |
+--------------------------+--------------------+-----------+-----+------+------+
|2001:db8::1ffe:0:0:0/112  |                    |eth2       |  -  |  V   |  V   |
```

```
|2001:db8::fd9a:0:1:0/112  |                    |eth3      |  -  |  V   |  V   |
+--------------------------+--------------------+----------+-----+------+------+


Routing Table Legend:

  V   - Route exists on the gateway and matches management information (if defined on the
management).
  -   - Route does not exist on the gateway.
 N/A  - Fetching Virtual Device configuration from the gateway failed.
 !NH  - Route exists on the gateway, but there is a Next Hop mismatch.

Note: Routes can be created automatically on the gateways by the Operating System.
Therefore, routes that appear on all gateways, but are not defined on the management,
do not necessarily indicate a problem.

Logging details are available at /opt/CPsuite-R82/fw1/log/vsx_util_20210625_18_11.log

[Expert@MGMT:0]#
```

vsx_util vsls

Description

Shows the configuration menu for Virtual System Load Sharing - status, redistribute, export, and import of configuration.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Important:

- The only mode available for a VSX Cluster that was installed as R81.10 and higher is **Virtual System Load Sharing (VSLS)**.
- The **High Availability** mode is available only if you upgrade a VSX Cluster from R81 or lower to R82.
  You can also convert a VSLS cluster to the High Availability mode (see *"Changing the VSX Cluster Type" on page 208*).

Syntax

```
vsx_util vsls
```

Required Input

- The applicable VSX Cluster object.
- The applicable redistribution option.

Comments

- Execute the command and follow the instructions on the screen.
- If the command output shows "`Operation not allowed. Object is not a Virtual System Load Sharing cluster.`", then run the *"vsx_util convert_cluster" on page 338* command.

Example

```
[Expert@MGMT:0]# vsx_util vsls
Enter Security Management Server/main Domain Management Server IP address (Hit 'ENTER' for
'localhost'): 172.16.16.240
Enter Administrator Name: admin
Enter Administrator Password:

Select VSX gateway/cluster object name:
  1)    VSX_Cluster_1
  2)    VSX_Cluster_2
  3)    VSX_GW_1
  4)    VSX_GW_2
Select: 1


VS Load Sharing - Menu
__________________________________
1. Display current VS Load sharing configuration
2. Distribute all Virtual Systems so that each cluster member is equally loaded
3. Set all VSes active on one member
4. Manually set priority and weight
5. Toggle VSLS mode between Active Up and Primary Up
6. Import configuration from a file
7. Export configuration to a file
8. Exit

Enter redistribution option (1-8) [1]:
```

vsx_provisioning_tool

This section describes the **VSX Provisioning Tool** (the `vsx_provisioning_tool` command).

Description

This tool allows the VSX administrator to add and remove Virtual Devices (Virtual Systems, Virtual Routers, Virtual Switches), interfaces and routes from the command line of a Security Management Server or Domain Management Server.

This allows the automation of the required VSX Provisioning operations in the environment.

Syntax

```
vsx_provisioning_tool -h
```

```
vsx_provisioning_tool [-s <Mgmt Server>] {-u <Username> | -c
<Certificate>} -p <Password>
      -o <Commands> [-a] -L
      -f <Input File> [-l <Line>] [-a] -L
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
`-s <Mgmt Server>`	Specifies the Security Management Server or the applicable Domain Management Server. Enter the IPv4 or IPv6 address, or the resolvable hostname name. This parameter is mandatory when you run the tool: ■ From a SmartConsole computer ■ On a Multi-Domain Server.
`-u <Username>`	Specifies the Management Server administrator's user name.
`-c <Certificate>`	Specifies the path and the name for the Management Server administrator's certificate file.

Parameter	Description
`-p <Password>`	Specifies the password of the: ■ Management Server administrator ■ Certificate file
`-o <Commands>`	Executes the commands you enter on the command line. See *"vsx_provisioning_tool Commands" on page 363*.
`-f <Input File>`	Specifies the path and the name for the file with the commands to execute. The tool treats all text begins with a hash sign (#) as a comment and ignores it. This way you can add comments on separate lines, or in-line. See: ■ *"Transactions" on page 362* ■ *"vsx_provisioning_tool Commands" on page 363*
`-l <Line>`	Specifies the line number in `<Input File>`, from which to start to execute the commands. You can use this "`-l`" parameter only together with the "`-f`" parameter.
`-a`	Specifies that before the tool executes the specified commands, it must make sure it can connect to all VSX Gateways. **Note** - This does not guarantee that a VSX Gateway can successfully apply all the specified commands.
`-L`	Specifies local authentication mode.

Exit Codes

Exit Code	Description
0	The tool successfully applied all changes, on all VSX Cluster Members.
1	The tool successfully applied all changes to the management database, but not to all VSX Cluster Members.
2	The tool successfully applied all changes, but SIC communication failed to establish with at least one VSX Cluster Member.
3	Connectivity test failed with at least one VSX Cluster Member (if you used the "-a" parameter). The tool did not apply changes to the management database, or to the VSX Cluster Member.
4	The tool failed to apply changes (due to internal error, syntax error, or another reason).

Note - If commands are executed from a file with multiple transactions, the exit code refers to the last transaction processed.

Example 1

Run the tool on the Security Management Server.

Execute the commands from the text `/var/log/vsx.txt` file.

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -f /var/log/vsx.txt
```

Example 2

Run the tool on the Multi-Domain Server in the context of the Domain Management Server called `MyDomain`.

Create a new Virtual System object called `VS1` on the VSX Cluster object called `VSXCluster1`

In the new Virtual System object, on the interface `eth4`, add a VLAN interface with VLAN ID 100 and IPv4 address 1.1.1.1/24.

```
mdsenv MyDomain
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add vd name VS1 vsx VSXCluster1, add interface name eth4.100 ip 1.1.1.1/24
```

Transactions

Notes:

- A transaction is a set of operations performed on one Virtual Device.
- The utility commits all operations to the management database together when the transaction ends.
  If the transaction fails, the utility discards all its commands.
- You must specify the name of the Virtual Device with a parameter in the first command.
  You do not need to specify this name again in other commands of the same transaction.
- You cannot send operations to different Virtual Devices in one transaction.
- You cannot start a new transaction until you exit the one before.
- When you send commands with the "`-o`" parameter, you can enter multiple commands (for example: add a Virtual System and then add interfaces and routes to it).
  Separate the commands with a comma (`,`).
  All the commands are one transaction.
  The "`-o`" parameter does not support explicit transaction commands.
- When you send commands with the "`-f`" parameter, you can use explicit transaction commands (see *"vsx_provisioning_tool Commands" on page 363*).
- Commands from a file can be one or more transactions:
  - If not inside a transaction, the current line is one transaction, which the utility automatically commits.
    You can write multiple commands in one line (as one transaction), separated with a comma (`,`).
  - If currently inside a transaction, the utility processes the lines, but does not take action until the transaction ends.

vsx_provisioning_tool Commands

All `vsx_provisioning_tool` commands are pairs of a key and a value.

The first two words in each command must appear in the correct order.

Other pairs can be written in any order.

Explicit Transaction Commands

Operation	Command Syntax
Begin a new transaction	`transaction begin`
End a transaction	`transaction end`
Cancel a transaction	`transaction cancel`

Note - SIC with the Virtual System is established automatically. If it fails, operations continue, and the transaction returns error code **2**.

Adding a VSX Gateway

Description

This command adds a new VSX Gateway object.

Syntax

```
add vsx type gateway name <Name of VSX Gateway Object> version
<Version> main_ip <Main IPv4 Address> [main_ip6 <Main IPv6
Address>] sic_otp <Activation Key> [rule_snmp {enable | disable}]
[rule_ssh {enable | disable}] [rule_ping {enable | disable} [rule_
ping6 {enable | disable}] [rule_https {enable | disable}] [rule_
drop {enable | disable}]
```

Note - In this transaction, you can only add the "`set physical interface`" command.

Parameters

`type`	`gateway`	You must use the value "`gateway`" to add a new VSX Gateway object.
`name <Name of VSX Gateway Object>`	Object name	Defines the name of the VSX Gatewayobject. You cannot use spaces of Check Point reserved words.
`version <Version>`	Check Point version	Defines the Check Point version of the VSX Gateway object. You must enter the exact version as appears in SmartConsole (case-sensitive).
`main_ip <Main IPv4 Address>`	IPv4 Address	Defines the main IPv4 Address of the VSX Gateway object.
`main_ip6 <Main IPv6 Address>`	IPv6 Address	Defines the main IPv6 Address of the VSX Gateway object.
`sic_otp <Activation Key>`	SIC password	You must enter the same Activation Key you entered during the First Time Configuration Wizard of the VSX Gateway.

`rule_snmp {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all SNMP packets sent to the VSX Gateway: ■ `enable` - Allows all SNMP packets ■ `disable` - Drops all SNMP packets (default)
`rule_ssh {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all SSH packets sent to the VSX Gateway: ■ `enable` - Allows all SSH packets ■ `disable` - Drops all SSH packets (default)
`rule_ping {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all ICMP Echo Request (ping) packets sent to the VSX Gateway: ■ `enable` - Allows all IPv4 ping packets ■ `disable` - Drops all IPv4 ping packets (default)
`rule_ping6 {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all ICMPv6 Echo Request (ping) packets sent to the VSX Gateway: ■ `enable` - Allows all IPv6 ping packets ■ `disable` - Drops all IPv6 ping packets (default)
`rule_https {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all HTTPS packets sent to the VSX Gateway: ■ `enable` - Allows all HTTPS packets ■ `disable` - Drops all HTTPS packets (default)
`rule_drop {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all packets (other than SNMP, SSH, ICMP, ICMPv6, HTTPS) sent to the VSX Gateway: ■ `enable` - Drops all other packets (default) ■ `disable` - Allows all other packets

Example

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add vsx name VSX_GW1 type gateway main_ip 192.168.20.1 version R82 sic_otp
ABCDEFG rule_ssh enable rule_ping enable
```

Adding a VSX Cluster

Description

This command adds a new VSX Cluster object.

Syntax

```
add vsx type cluster name <Name of VSX Cluster Object> version
<Version> main_ip <Main Virtual IPv4 Address> main_ip6 <Main
Virtual IPv6 Address> cluster_type {vsls | ha | crbm} sync_if_name
<Name of Sync Interface> sync_netmask <Sync Interface Netmask>
[rule_snmp {enable | disable}] [rule_ssh {enable | disable}]
[rule_ping {enable | disable} [rule_ping6 {enable | disable}]
[rule_https {enable | disable}] [rule_drop {enable | disable}]
```

Important - You must run the "`add vsx_member`" command for each VSX Cluster Member in the same transaction as the "`add vsx type cluster name`" command.

Syntax

```
add vsx_member name <Member Name> [main_ip <Member Main
IPv4 Address>] [main_ip6 <Member Main IPv6 Address>] sync_
ip <Sync Interface IPv4 Address> sic_otp <SIC Password>
```

Parameters

Parameter	Value	Notes
`type`	`cluster`	You must use the value "`cluster`" to add a new VSX Cluster object.
`name <Name of VSX Cluster Object>`	Object name	Defines the name of the VSX Cluster object. You cannot use spaces of Check Point reserved words.
`version <Version>`	Check Point version	Defines the Check Point version of the VSX Cluster object. You must enter the exact version as appears in SmartConsole (case-sensitive).
`main_ip <Main Virtual IPv4 Address>`	IPv4 Address	Defines the main IPv4 Virtual Address of the VSX Cluster object.

Parameter	Value	Notes
`main_ip6 <Main Virtual IPv6 Address>`	IPv6 Address	Defines the main IPv6 Virtual Address of the VSX Cluster object.
`cluster_type {vsls | ha | crbm}`	Cluster type	Defines the cluster type. Enter one of these: ■ `vsls` - Virtual System Load Sharing mode ■ `ha` - High Availability mode ■ `crbm` - X-Series appliances (former BlueCoat / Crossbeam)
`sync_if_name <Name of Sync Interface>`	Sync interface name	Defines the name of the Cluster Synchronization interface.
`sync_netmask <Sync Interface Netmask>`	IPv4 Network mask	Defines an IPv4 Netmask for the Cluster Synchronization interface (in a dot-quad format X.X.X.X).
`rule_snmp {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all SNMP packets sent to the VSX Cluster Members: ■ `enable` - Allows all SNMP packets ■ `disable` - Drops all SNMP packets (default)
`rule_ssh {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all SSH packets sent to the VSX Cluster Members: ■ `enable` - Allows all SSH packets ■ `disable` - Drops all SSH packets (default)
`rule_ping {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all ICMP Echo Request (ping) packets sent to the VSX Cluster Members: ■ `enable` - Allows all IPv4 ping packets ■ `disable` - Drops all IPv4 ping packets (default)

Parameter	Value	Notes
`rule_ping6 {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all ICMPv6 Echo Request (ping) packets sent to the VSX Cluster Members: ■ `enable` - Allows all IPv6 ping packets ■ `disable` - Drops all IPv6 ping packets (default)
`rule_https {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all HTTPS packets sent to the VSX Cluster Members: ■ `enable` - Allows all HTTPS packets ■ `disable` - Drops all HTTPS packets (default)
`rule_drop {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all packets (other than SNMP, SSH, ICMP, ICMPv6, HTTPS) sent to the VSX Cluster Members: ■ `enable` - Drops all other packets (default) ■ `disable` - Allows all other packets

Example

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add vsx name VSX1 type cluster cluster_type vsls main_ip 192.168.1.1 version
R82 sync_if_name eth3 sync_netmask 255.255.255.0 rule_ssh enable rule_ping enable
```

Adding a Virtual Device

Description

This command adds a new Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Syntax

```
add vd name <Name of Virtual Device Object> vsx <Name of VSX
Gateway or VSX Cluster Object > [type {vs | vsbm | vsw | vr}] [vs_
mtu <MTU>] [instances <Number of IPv4 CoreXL Firewall instances>]
[instances6 <Number of IPv6 CoreXL Firewall instances>] [main_ip
<Main IPv4 Address>] [main_ip6 <Main IPv6 Address>] [calc_topo_
auto {true | false}]
```

Parameters

Parameter	Value	Notes
`name <Name of Virtual Device Object>`	Object name	Defines the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`vsx <Name of VSX Gateway or VSX Cluster Object >`	Parent object name	Defines the name of the applicable VSX Gateway or VSX Cluster object, in which you create this Virtual Device. You cannot use spaces or Check Point reserved words. Mandatory parameter.
`type {vs | vsbm | vsw | vr}`	Type of Virtual Device	Defines the type of the Virtual Device: ■ `vs` - Virtual System (default) ■ `vsbm` - Virtual System in Bridge Mode ■ `vsw` - Virtual Switch ■ `vr` - Virtual Router

Parameter	Value	Notes
`vs_mtu <MTU>`	Integer	Defines the Global MTU value for all interfaces. This parameter is applicable only for a: ■ Virtual System in Bridge Mode (`type vsbm`) ■ Virtual Switch (`type vsw`) Default is 1500 bytes. **Note** - For a Virtual Switch, if you do not add a VLAN or physical interface in the same transaction, the utility ignores this value.
`instances <Number of IPv4 CoreXL Firewall instances>`	Integer	Defines the number of IPv4 CoreXL Firewall instances. This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual System in Bridge Mode (`type vsbm`) Default is 1. For more information about CoreXL, see *R82 Performance Tuning Administration Guide*.
`instances6 <Number of IPv6 CoreXL Firewall instances>`	Integer	Defines the number of IPv6 CoreXL Firewall instances. This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual System in Bridge Mode (`type vsbm`) Default is 1. For more information about CoreXL, see *R82 Performance Tuning Administration Guide*.

Parameter	Value	Notes
`main_ip <Main IPv4 Address>`	IPv4 Address	Defines the main IPv4 Address of the Virtual Device object. This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual Router (`type vr`) **Note** - If you do not specify this value explicitly, the utility uses the IPv4 address of the first interface added to the new device.
`main_ip6 <Main IPv6 Address>`	IPv6 Address	Defines the main IPv6 Address of the Virtual Device object. This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual Router (`type vr`) **Note** - If you do not specify this value explicitly, the utility uses the IPv6 address of the first interface added to the new device.
`calc_topo_auto {true | false}`	■ `true` ■ `false`	Defines how to calculate topology based on routes: ■ `true` - Automatically calculate topology based on routes (default) ■ `false` - Does not calculate topology based on routes (administrator can configure it manually) This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual Router (`type vr`)

Example - Adding a Virtual Switch "VirtSwitch1" to the VSX Gateway "VSX_GW1"

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add vd name VirtSwitch1 vsx VSX_GW1 type vsw
```

Deleting a Virtual Device

Description

This command deletes a Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

You cannot delete a Virtual Device if:

- It is referenced by a policy rule.
- It is referenced by other objects.
- It is enabled for global use in a Multi-Domain Security Management environment.

Important - After you delete a Virtual Device, you cannot have more commands in the same transaction.

Syntax

```
remove vd name <Name of Virtual Device Object>
```

Parameters

Parameter	Value	Notes
`name <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.

Example

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o remove vd name VirtSwitch1
```

Modifying Settings of a Virtual Device

Description

This command changes the settings of an existing Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Syntax

```
set vd name <Name of Virtual Device Object> [vs_mtu <MTU>]
[instances <Number of IPv4 CoreXL Firewall instances>] [instances6
<Number of IPv6 CoreXL Firewall instances>] [main_ip <Main IPv4
Address>] [main_ip6 <Main IPv6 Address>] [calc_topo_auto {true |
false}]
```

Parameters

Parameter	Value	Notes
`name <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`vs_mtu <MTU>`	Integer	Specifies the Global MTU value for all interfaces. This parameter is applicable only for a: ▪ Virtual System in Bridge Mode ▪ Virtual Switch Default is 1500 bytes.

Parameter	Value	Notes
`instances <Number of IPv4 CoreXL Firewall instances>`	Integer	Specifies the number of IPv4 CoreXL Firewall instances. This parameter is applicable only for a: ■ Virtual System ■ Virtual System in Bridge Mode Default is 1. For more information about CoreXL, see *R82 Performance Tuning Administration Guide*.
`instances6 <Number of IPv6 CoreXL Firewall instances>`	Integer	Specifies the number of IPv6 CoreXL Firewall instances. This parameter is applicable only for a: ■ Virtual System ■ Virtual System in Bridge Mode Default is 1. For more information about CoreXL, see *R82 Performance Tuning Administration Guide*.
`main_ip <Main IPv4 Address>`	IPv4 Address	Specifies the main IPv4 Address of the Virtual Device object. This parameter is applicable only for a: ■ Virtual System ■ Virtual Router **Note** - To remove the current IPv4 address, set the value to "`empty`". For example: `set vd name VS1 main_ip empty`
`main_ip6 <Main IPv6 Address>`	IPv6 Address	Specifies the main IPv6 Address of the Virtual Device object. This parameter is applicable only for a: ■ Virtual System ■ Virtual Router **Note** - To remove the current IPv6 address, set the value to `empty`. For example: `set vd name VS1 main_ip6 empty`

Parameter	Value	Notes
`calc_topo_auto {true | false}`	■ `true` ■ `false`	Specifies how to calculate topology based on routes: ■ `true` - Automatically calculate topology based on routes (default) ■ `false` - Does not calculate topology based on routes (administrator can configure it manually) This parameter is applicable only for a: ■ Virtual System ■ Virtual Router

Example

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o set vd name VS1 instances 8 main_ip 192.0.2.6 calc_topo_auto false
```

Adding a Physical or VLAN Interface to a Virtual Device

Description

This command adds an interface to an existing Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Syntax

```
add interface vd <Name of Virtual Device Object> {name <Name of
Interface> | leads_to <Name of VSW or VR Object>} ip <IPv4
Address>{/<IPv4 Prefix Length> | netmask <IPv4 Netmask> | prefix
<IPv4 Prefix>} ip6 <IPv6 Address>{/<IPv6 Prefix Length> | netmask6
<IPv6 Netmask> | prefix6 <IPv6 Prefix>} [propagate {true | false}]
[propagate6 {true | false}] [topology {external | internal_
undefined | internal_this_network | internal_specific [specific_
group <Name of Network Group Object>]}] [mtu <MTU>]
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`name <Name of Interface>`	Interface name	Specifies the name of the physical or VLAN interface. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.
`leads_to <Name of VSW or VR Object>`	Object name	Specifies the name of the Virtual Switch or Virtual Router object, to which this interface connects. This parameter is applicable only for a Virtual System. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.

Parameter	Value	Notes
`ip <IPv4 Address> {/<IPv4 Prefix> | netmask <IPv4 Netmask> | prefix <IPv4 Prefix>}`	IPv4 configuration	Specifies the IPv4 settings: ■ `<IPv4 Address>` - IPv4 address ■ `<IPv4 Prefix>` - Integer between 1 and 32 ■ `<IPv4 Netmask>` - Number in a format X.X.X.X This parameter is applicable only for a: ■ Virtual System ■ Virtual Router For interfaces on a Virtual System that connect to a Virtual Router, you must use the possible maximum for the IPv4 address family: ■ Netmask 255.255.255.255 ■ Prefix 32
`ip6 <IPv6 Address> {/<IPv6 Prefix> | netmask6 <IPv6 Netmask> | prefix6 <IPv6 Prefix>}`	IPv6 configuration	Specifies the IPv6 settings: ■ `<IPv6 Address>` - IPv6 address ■ `<IPv6 Prefix>` - Integer between 64 and 128 ■ `<IPv6 Netmask>` - Number in a format XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX This parameter is applicable only for a: ■ Virtual System ■ Virtual Router For interfaces on a Virtual System that connect to a Virtual Router, you must use the possible maximum for the IPv6 address family: ■ Netmask FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF ■ Prefix 128

Parameter	Value	Notes
`propagate {true | false}`	▪ `true` ▪ `false`	Controls how to propagate the IPv4 routes to adjacent Virtual Devices: ▪ `true` - Propagate the IPv4 routes ▪ `false` - Do not propagate the IPv4 routes (default) **Note** - This parameter is applicable only for a Virtual System with VLAN or physical interfaces.
`propagate6 {true | false}`	▪ `true` ▪ `false`	Controls how to propagate the IPv6 routes to adjacent Virtual Devices: ▪ `true` - Propagate the IPv6 routes ▪ `false` - Do not propagate the IPv6 routes (default) **Note** - This parameter is applicable only for a Virtual System with VLAN or physical interfaces.
`topology {external | internal_undefined | internal_this_network | internal_specific }`	▪ `external` ▪ `internal_undefined` ▪ `internal_this_network` ▪ `internal_specific`	Specifies the Topology configuration of the interface: ▪ `external` - External interface. ▪ `internal_undefined` - Internal interface with undefined topology. This is the default for a Virtual System in Bridge Mode. ▪ `internal_this_network` - Internal interface. This is the default for a Virtual System and Virtual Router. Virtual System in Bridge Mode does not support this topology. ▪ `internal_specific [specific_group <Name of Network Group Object>]` - Internal interface with topology defined by the specified Network Group object. This parameter is applicable only for a: ▪ Virtual System ▪ Virtual System in Bridge Mode ▪ Virtual Router

Parameter	Value	Notes
`specific_group <Network Group Object Name>`	Name of Network Group Object	If you specified the "`topology internal_specific`" parameter, then specify the name of the Network Group object that contains the applicable Network objects. **Note** - This parameter is applicable only if you disable the automatic topology calculation with the "`set vd ... calc_topo_auto false`" command (see *"Modifying Settings of a Virtual Device" on page 375*).
`mtu <MTU>`	Integer	Specifies the MTU value for this interface. Default is 1500 bytes. This parameter is applicable only for a: ■ Virtual System ■ Virtual Router

Example - Add VLAN interface eth4.100 with IPv4 1.1.1.1/24 to the Virtual System 'VirtSystem1'

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add interface vd VirtSystem1 name eth4.100 ip 1.1.1.1/24
```

Adding a Bridge Interface to a Virtual System

Description

Some Software Blades and features are not supported on a Virtual System in Bridge Mode, because it may not have an IP address.

For example: Threat Emulation, Identity Awareness, Identity Awareness Captive Portal, and UserCheck Portal are not supported.

This command adds a Bridge interface to an existing regular Virtual System object that always has an IP address.

As a result, the Virtual System can support these Software Blades and features for the traffic that passes over the configured bridge interface.

Notes:

- Names of bridge interfaces have a template "`brX`", where "`X`" is a digit.
- It is necessary to add subordinate interfaces in pairs to a bridge interface.
- To see the bridge interfaces you configured in the Virtual System object:
  1. Connect to the command line on the VSX Gateway (each VSX Cluster Member).
  2. Log in to the Expert mode.
  3. Go to the context of the Virtual System:
     ```
     vsenv <VSID>
     ```
  4. Examine the list of interfaces:
     ```
     ifconfig
     ```
- You can delete bridge interfaces from a Virtual System either in SmartConsole, or with the "`vsx_provisioning_tool`" command (see *"Removing an Interface from a Virtual Device" on page 386*).

Syntax

```
attach bridge vd <Name of Virtual System Object> ifs1 <Name of First Subordinate Interface> ifs2 <Name of Second Subordinate Interface>
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual System Object>`	Object name	Specifies the name of the Virtual System object. Mandatory parameter, if this is the first command in a transaction.
`ifs1 <Name of First Subordinate Interface>`	Interface name	Specifies the name of the physical interface to be the first subordinate interface of a bridge interface. **Note** - This physical interface must not have an IP address
`ifs2 <Name of First Second Interface>`	Interface name	Specifies the name of the physical interface to be the second subordinate interface of a bridge interface. **Note** - This physical interface must not have an IP address

Example 1 - Adding a Bridge interface with subordinate interfaces "eth2" and "eth3" in the Virtual System "VS1"

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o attach bridge vd VS1 ifs1 eth2 ifs2 eth3
```

Example 2 - Adding a Multi Bridge interface in the Virtual System "VS1"

In this example, we add pairs of VLAN interfaces to the Virtual System "VS1" to add a Multi Bridge interface (see *"Multi Bridge Interfaces" on page 276*):

- VLANs eth2.403 and eth3.403 as the first bridge interface
- VLANs eth2.504 and eth3.504 as the second bridge interface

The prerequisite is to configure both physical interfaces "eth2" and "eth3" as VLAN Trunks (see *"Configuring a Physical Interface as VLAN Trunk" on page 392*).

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o attach bridge vd VS1 ifs1 eth2.403 ifs2 eth3.403, attach bridge ifs1
eth2.504 ifs2 eth3.504
```

Adding a VPN Tunnel Interface to a Virtual Device

Description

Virtual Tunnel Interface (VTI) is a virtual interface that is used for establishing a Route-Based VPN tunnel.

This command adds a VTI to an existing Virtual System object.

The VPN tunnel and its properties are defined by the VPN community that contains the two Security Gateways.

You must define the VPN community and its member Security Gateways before you can create a VTI.

To learn more about Route Based VPN, see the *R82 Site to Site VPN Administration Guide* > Chapter *Route Based VPN*.

Syntax

```
add interface vd <Name of Virtual System Object> vpn_tunnel
numbered peer <Name of VPN Peer Object> local <Tunnel Local IP>
remote <Tunnel Remote IP> [tunnel_id <Tunnel ID>]
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual System Object>`	Object name	Specifies the name of the Virtual System object (as configured in SmartConsole). Mandatory parameter, if this is the first command in a transaction.
`vpn_tunnel numbered`	▪ `true` ▪ `false`	Specifies the type of the VPN tunnel as numbered. Uses a specified, static IPv4 addresses for local and remote connections.
`peer <Name of VPN Peer Object>`	Object name	Specifies the name of the remote peer object as defined in the VPN community in SmartConsole.

Parameter	Value	Notes
`local <Tunnel Local IP> remote <Tunnel Remote IP>`	IPv4 configuration	Specifies the IPv4 addresses in dotted decimal format for the VPN tunnel endpoints: ■ `local <Tunnel Local IP>` - IPv4 address of the VPN tunnel on this Virtual System ■ `remote <Tunnel Remote IP>` - IPv4 address of the VPN tunnel on the remote VPN peer Applies to the Numbered VTI only.
`tunnel_id <Tunnel ID>`	Integer	Specifies the unique Tunnel ID (integer from 1 to 32768). **Note** - If the specified ID is already used by another VPN tunnel on this VSX Gateway or VSX Cluster Member, this parameter is ignored and the next available ID is used instead.

Example - Numbered VTI

```
vsx_provisioning_tool -o add interface vd vs1 vpn_tunnel numbered peer AWS_Peer local 169.254.46.238 remote 169.254.46.237 tunnel_id 10
```

Note - Unnumbered VTIs are not supported.

Removing an Interface from a Virtual Device

Description

This command removes an interface from an existing Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Important:

- If the interface you remove leads to a Virtual Router, all routes through that interface are removed automatically.
- You must remove **all** subordinate interfaces of a bridge interface in the same transaction. This also removes the bridge interface.

Note - If there are routes that have a next-hop IP address, which would become inaccessible without this interface, the transaction fails.

Syntax

```
remove interface vd <Name of Virtual Device Object> {name <Name of Interface> | leads_to <Name of VSW or VR Object>}
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`name <<Name of Interface>>`	Interface name	Specifies the name of the physical or VLAN interface. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.
`leads_to <Name of VSW or VR Object>`	Object name	Specifies the name of the Virtual Switch or Virtual Router object, to which this interface connects. This parameter is applicable only for a Virtual System. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.

Example 1 - Removing a VLAN interface from a Virtual System "VS1"

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o remove interface vd VS1 name eth4.100
```

Example 2 - Removing all subordinate interfaces "eth2" and "eth3" of a bridge interface in the Virtual System "VS1"

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o remove interface vd VS1 name eth2, remove interface vd VS1 name eth3
```

Modifying Settings of an Interface

Description

This command changes the settings of an interface that belongs to an existing Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Note - You cannot change or remove the IP address or netmask of an existing interface with this command. You can remove the interface and add a new interface with a different IP address, but not all the previous interface settings are kept.

Syntax

```
set interface vd <Name of Virtual Device Object> {name <Name of Interface> [new_name <Name of New Interface>] | leads_to <Name of VSW or VR Object> [new_leads_to <Name of New VSW or VR Object>]} [propagate {true | false}] [propagate6 {true | false}] [topology {external | internal_undefined | internal_this_network | internal_specific [specific_group <Network Group Object Name>]}] [mtu <MTU>]
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`name <Name of Interface>`	Interface name	Specifies the name of the physical or VLAN interface. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.

Parameter	Value	Notes
`new_name <Name of New Interface>`	Interface name	You can change the name, but not the type of interface. **Note** - You can change a VLAN or physical interface only to a VLAN or physical interface.
`leads_to <Name of VSW or VR Object>`	Object name	Specifies the name of the Virtual Switch or Virtual Router object, to which this interface connects. This parameter is applicable only for a Virtual System. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.
`new_leads_to <Name of New VSW or VR Object>`	Object name	You can where the interface leads: ■ You can change an interface that leads to a Virtual Switch only to lead to a different Virtual Switch. ■ You can change an interface that leads to a Virtual Router only to lead to a different Virtual Router.
`propagate {true | false}`	■ `true` ■ `false`	Controls how to propagate the IPv4 routes to adjacent Virtual Devices: ■ `true` - Propagate the IPv4 routes ■ `false` - Do not propagate the IPv4 routes (default) **Note** - This parameter is applicable only for a Virtual System with VLAN or physical interfaces.

Parameter	Value	Notes
`propagate6 {true | false}`	■ `true` ■ `false`	Controls how to propagate the IPv6 routes to adjacent Virtual Devices: ■ `true` - Propagate the IPv6 routes ■ `false` - Do not propagate the IPv6 routes (default) **Note** - This parameter is applicable only for a Virtual System with VLAN or physical interfaces.
`topology {external | internal_undefined | internal_this_network | internal_specific}`	■ `external` ■ `internal_undefined` ■ `internal_this_network` ■ `internal_specific`	Specifies the Topology configuration of the interface: ■ `external` - External interface. ■ `internal_undefined` - Internal interface with undefined topology. This is the default for Virtual System in Bridge Mode. ■ `internal_this_network` - Internal interface. This is the default for Virtual System and Virtual Router. Virtual System in Bridge Mode does not support this topology. ■ `internal_specific [specific_group <Network Group Object Name>]` - Internal interface with topology defined by the specified Network Group object. This parameter is applicable only for a: ■ Virtual System ■ Virtual System in Bridge Mode ■ Virtual Router

Parameter	Value	Notes
`specific_group <Network Group Object Name>`	Name of Network Group Object	If you specified the "`topology internal_specific`" parameter, then specify the name of the Network Group object that contains the applicable Network objects. **Note** - This parameter is applicable only if you disable the automatic topology calculation with the "`set vd ... calc_topo_auto false`" command (see *"Modifying Settings of a Virtual Device" on page 375*).
`mtu <MTU>`	Integer	Specifies the MTU value for this interface. Default is 1500 bytes. This parameter is applicable only for: ■ Virtual System ■ Virtual Router

Example - On the Virtual System "VS1", change the VLAN interface eth4.10 to the physical interface eth5

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o set interface vd VS1 name eth4.100 new_name eth5 propagate true topology
internal_specific specific_group NYGWs
```

Configuring a Physical Interface as VLAN Trunk

Description

This command configures a physical interface as VLAN Trunk.

This is required to configure VLAN interfaces the physical interface.

Important - Make sure the physical interface you configure as VLAN Trunk does not have an IP address.

Syntax

```
set physical_interface vd <Name of VSX Gateway or VSX Cluster Object> name <Name of Interface> vlan_trunk {true | false}
```

Parameters

Parameter	Value	Notes
`vd <Name of VSX Gateway or VSX Cluster Object>`	Object name	Specifies the name of the VSX Gateway or VSX Cluster object. Mandatory parameter, if this is the first command in a transaction.
`name <Name of Interface>`	Interface name	Specifies the name of the physical interface.
`vlan_trunk {true | false}`	■ `true` ■ `false`	Controls whether this physical interface is a VLAN Trunk: ■ `true` - VLAN Trunk interface ■ `false` - Regular physical interface (default)

Example - On the VSX Gateway "VSX1" configure the physical interface eth2 as VLAN Trunk

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o set physical_interface vd VSX1 name eth2 vlan_trunk true
```

Adding a Route

Description

This command adds an IPv4 or IPv6 route to an existing Virtual System or Virtual Router object.

Note - This command detects IPv4 and IPv6 automatically.

Syntax

```
add route vd <Name of VS or VR Object> destination {<IP Address>
[/<IP Prefix>] | default | default6} [{netmask <IP Netmask> |
prefix <IP Prefix>}] {next_hop <Next Hop IP Address> | leads_to
<Name of VS or VR Object>} [propagate {true | false}]
```

Parameters

Parameter	Value	Notes
`vd <Name of VS or VR Object>`	Object name	Specifies the name of the Virtual System or Virtual Router object. Mandatory parameter, if this is the first command in a transaction.
`destination {<IP Address> [/<IP Prefix>] | default | default6}`	See the *Notes* column on the right	Specifies the route destination settings: ■ `<IP Address>` - IPv4 or IPv6 address ■ `<IP Prefix>` - • For IPv4 - Integer between 1 and 32 • For IPv6 - Integer between 64 and 128 ■ `default` - Use the default IPv4 route ■ `default6` - Use the default IPv6 route
`netmask <IP Netmask>`	Number	Specifies an IP Netmask: ■ For IPv4 - Number in a format X.X.X.X ■ For IPv6 - Number in a format XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
`prefix <IP Prefix>`	Integer	Specifies the IP address prefix length: ■ For IPv4 - Integer between 1 and 32 ■ For IPv6 - Integer between 64 and 128

Parameter	Value	Notes
`next_hop <Next Hop IP Address>`	IP Address	Specifies the IP address of the next hop of the route. **Notes:** ■ This IP address must be on a subnet of an existing interface. ■ You must use the "`next_hop`" or "`leads_to`" parameter, but not both.
`leads_to <Name of VS or VR Object>`	Object name	Specifies the name of the Virtual System or Virtual Router object, which is the next hop for the configured route. **Note** - You must use the "`next_hop`" or "`leads_to`" parameter, but not both.
`propagate {true | false}`	■ `true` ■ `false`	Controls how to propagate the IP routes to adjacent Virtual Devices: ■ `true` - Propagate the IP routes ■ `false` - Do not propagate the IP routes (default) **Note** - The "`propagate`" parameter is applicable only if you specified the "`next_hop`" parameter.

Example - Adding a route on the Virtual System "VS1" that uses the default IPv4 route as a destination and the Virtual Router "VR3" as a next hop

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add route vd VS1 destination default leads_to VR3
```

Removing a Route

Description

This command removes an IPv4 or IPv6 route from an existing Virtual System or Virtual Router object.

Note - This command detects IPv4 and IPv6 automatically.

Syntax

```
remove route vd <Name of VS or VR Object> destination {<IP
Address>[/<IP Prefix>] | default | default6} [{netmask <IP
Netmask> | prefix <IP Prefix>]
```

Parameters

Parameter	Value	Notes
`vd <Name of VS or VR Object>`	Object name	Specifies the name of the Virtual System or Virtual Router object. Mandatory parameter, if this is the first command in a transaction.
`destination {<IP Address> [/<IP Prefix>] | default | default6}`	See the *Notes* column on the right	Specifies the route destination settings: ■ `<IP Address>` - IPv4 or IPv6 address ■ `<IP Prefix>` - • For IPv4 - Integer between 1 and 32 • For IPv6 - Integer between 64 and 128 ■ `default` - Use the default IPv4 route ■ `default6` - Use the default IPv6 route
`netmask <IP Netmask>`	Number	Specifies an IP Netmask: ■ For IPv4 - Number in a format X.X.X.X ■ For IPv6 - Number in a format XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
`prefix <IP Prefix>`	Integer	Specifies the IP address prefix length: ■ For IPv4 - Integer between 1 and 32 ■ For IPv6 - Integer between 64 and 128

Example - Removing a route from the Virtual System "VS1" that uses the default IPv6 route as a destination

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o remove route vd VS1 destination default6
```

Showing Virtual Device Data

Description

This command shows the information about an existing Virtual Device object.

Syntax

```
show vd name <Name of Virtual Device Object>
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual Device Object>`	Name of the Virtual Device	Specifies the name of the Virtual Device object. Mandatory parameter.

Comments

- The command shows only non-automatic routes.
- The command does not show routes that are created automatically with route propagation.
- For a Virtual Router and Virtual Switch:

  The command does not show the `wrpj` interfaces (created automatically) that connect to Virtual Systems.

Script Examples

Note - Line numbers in the left column are written only to make it easier to read the script examples.

Example 1

Create a Virtual System connected to a Virtual Router.

Add a default route on the Virtual System that routes the traffic to the Virtual Router.

Add applicable routes on the Virtual Router to route the traffic to the Virtual System.

Line	Command
1	`transaction begin`
2	`add vd name VR1 vsx VSX1 type vr`
3	`add interface name eth3.100 ip 10.0.0.1/24`
4	`transaction end`
5	`transaction begin`
6	`add vd name VR2 vsx VSX2 type vr`
7	`add interface name eth3.200 ip 20.0.0.1/24`
8	`transaction end`
9	`transaction begin`
10	`add vd name VS1 vsx VSX1`
11	`add interface leads_to VR1 ip 192.168.1.1/32`
12	`add interface name eth4.20 ip 192.168.20.1/24 propagate true`
13	`add route destination default leads_to VR1`
14	`add route destination 192.168.40.0/25 next_hop 192.168.20.254`
15	`transaction end`

Example 2

Create a Virtual System connected to a Virtual Switch, with manual topology.

Line	Command
1	`transaction begin`
2	`add vd name VSW1 vsx VSX1 type vsw vs_mtu 1400`
3	`add interface name eth3.100`
4	`transaction end`
5	`transaction begin`
6	`add vd name VS1 vsx VSX1 calc_topo_auto false`
7	`add interface leads_to VSW1 ip 10.0.0.1/24 ip6 2001::1/64 topology external`
8	`add interface name eth4.20 ip 192.168.20.1/25 ip6 2020::1/64 topology internal_this_network`
9	`add route destination default next_hop 10.0.0.254`
10	`add route destination default6 next_hop 2001::254`
11	`transaction end`

Example 3

Add CoreXL Firewall instances to the Virtual System made in the last example.

Turn on automatic calculation of topology.

Change the name of the internal interface, and decrease its MTU.

Line	Command
1	`transaction begin`
2	`set vd name VS1 instances 4 instances6 2 calc_topo_auto true`
3	`set interface name eth4.20 new_name eth4.21 mtu 1400`
4	`transaction end`

Configuration Examples

This section provides examples of VSX configuration.

Example 1: VSX Gateway managed by Security Management Server

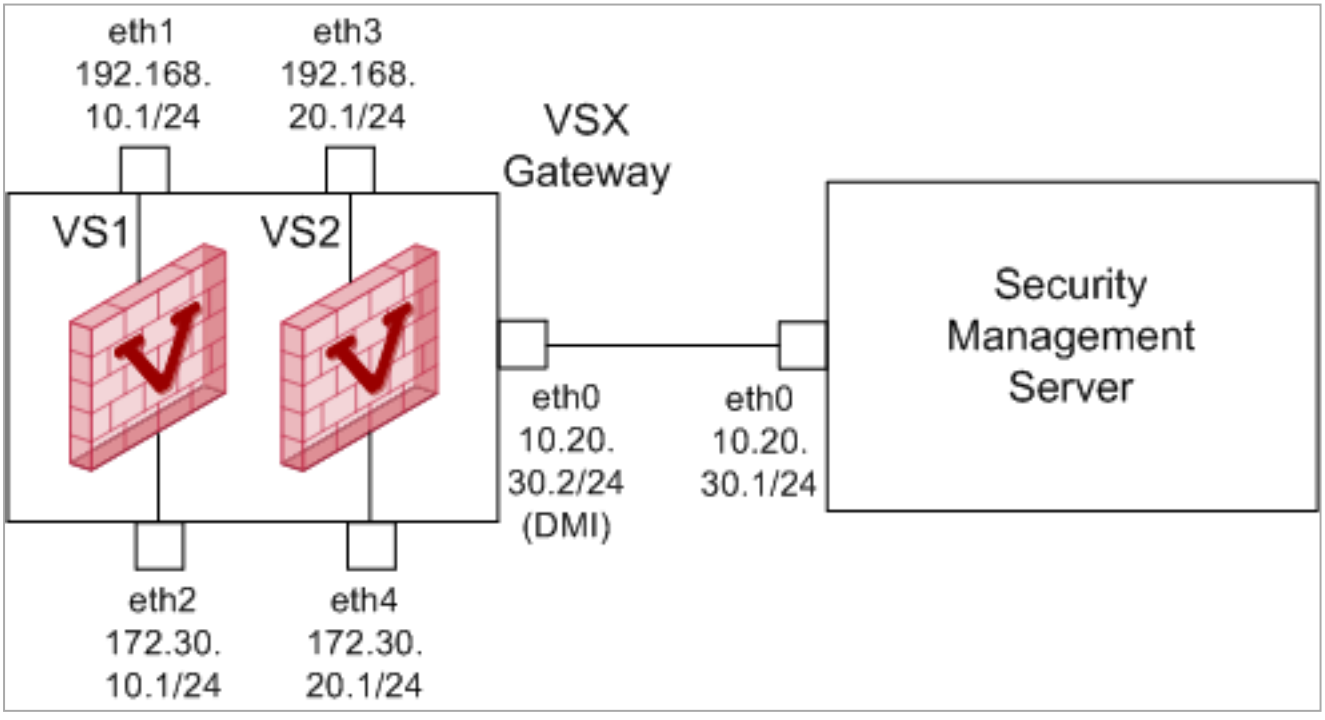
This example shows:

- One VSX Gateway with DMI management connection FIPS
- Two Virtual Systems:
  - Each Virtual System connects directly to available physical interfaces on the VSX Gateway
  - One Virtual System is configured with the IPsec VPN Software Blade
  - One Virtual System is configured with the Mobile Access Software Blade
- One Security Management Server manages both the VSX Gateway and the two Virtual Systems.

Related documentation:

- *R82 Installation and Upgrade Guide*
- *R82 Gaia Administration Guide*
- *R82 Security Management Administration Guide*

Topology



Action Plan

1. **Install the Security Management Server**

   See the *R82 Installation and Upgrade Guide*.

Step	Instructions
A	Install a Check Point appliance or Open Server.
B	Install Gaia OS.
C	Run the Gaia First Time Configuration Wizard. These settings are specific to the Security Management Server: a. On the **Management Connection** page, select the applicable interface and configure the applicable IPv4 address. In our example: `eth0, 10.20.30.1/24` b. On the **Installation Type** page, select **Security Gateway and/or Security Management**. c. On the **Products** page, select **Security Management**.
D	Install the applicable licenses.
E	Configure the Security Management Server: a. Connect with SmartConsole to the Security Management Server. b. Configure the applicable Management Software Blades and settings. c. Publish the SmartConsole session.

2. **Install the VSX Gateway**

   See the *R82 Installation and Upgrade Guide*.

Step	Instructions
A	Install a Check Point appliance or Open Server.
B	Install Gaia OS.

Step	Instructions
C	Run the Gaia First Time Configuration Wizard. These settings are specific to the VSX Gateway: a. On the **Management Connection** page, select the interface for the DMI management connection and configure the applicable IPv4 address. In our example: `eth0, 10.20.30.2/24` b. On the **Internet Connection** page, do **not** configure IP addresses on physical interfaces, to which your Virtual Systems connect directly. c. On the **Installation Type** page, select **Security Gateway and/or Security Management**. d. On the **Products** page, select **Security Gateway**. e. On the **Dynamically Assigned IP** page, select **No**.
D	Make sure to enable the applicable physical interfaces: To enable a physical interface in Gaia Portal a. Connect to the Gaia Portal in your web browser. In our example: `https://10.20.30.2` b. Click **Network Management > Network Interfaces**. c. In the upper left corner, click the lock icon to obtain the configuration lock. d. Select the applicable physical interface > click **Edit**. e. Select **Enable**. f. Click **OK**. To enable a physical interface in Gaia Clish, run: a. `set interface <`*Name of Physical Interface*`> state on` b. `save config`
E	Install the applicable licenses.

3. **Create the VSX Gateway object in SmartConsole**

   See *"Configuring VSX Gateways" on page 98*.

Step	Instructions
A	At the top, click **Objects > More object types > Network Object > Gateways and Servers > VSX > New Gateway**.

Step	Instructions
B	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 object. In our example: `MyVsxGw` b. In the **Enter the VSX Gateway IPv4** field, enter the same IPv4 address you configured during the First Time Configuration Wizard of the VSX Gateway on the **Management Connection** page. In our example: `10.20.30.1/24` c. In the **Enter the VSX Gateway IPv6** field, enter the same IPv6 address you configured during the First Time Configuration Wizard of the VSX Gateway on the **Management Connection** page. d. In the **Select the VSX Gateway Version** field, select the Check Point version. In our example: `R82` e. Click **Next**.
C	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 First Time Configuration Wizard of the VSX Gateway. 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 VSX Gateway. b. Make sure there is a physical connectivity between the VSX Gateway 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. On the **VSX Gateway General Properties** page, click **Reset**. g. Enter the same Activation Key you entered in the `cpconfig` menu. h. Click **Initialize**.

Step	Instructions
D	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 VSX Gateway. b. If you plan to connect more than one Virtual System directly to same physical interface, you must select **VLAN Trunk** for that physical interface. c. Click **Next**.
E	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 Network Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router. b. Click **Next**.
F	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.
G	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**.
H	Examine the VSX configuration: a. Connect to the command line on the VSX Gateway. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

4. **Configure the VSX Gateway object in SmartConsole**

See *"Working with VSX Gateways" on page 104*.

Step	Instructions
A	From the left navigation toolbar, click **Gateways & Servers**.

Step	Instructions
B	Open the VSX Gateway object. In our example: `MyVsxGw`
C	Enable the applicable Software Blades. 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 R82 Home Page.
D	Configure other applicable settings.
E	Click **OK** to push the updated VSX Configuration. Click **View Report** for more information.
F	Install policy on the VSX Gateway object: a. Click **Install Policy**. The **Install Policy** window opens. b. In the **Policy** field, select the default policy for this VSX Gateway object. This policy is called: `<Name of VSX Gateway object>_VSX`. In our example: `MyVsxGw_VSX` c. Click **Install**.
G	Examine the VSX configuration: a. Connect to the command line on the VSX Gateway. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

5. **Create the first Virtual System object in SmartConsole**

   See *"Working with Virtual Systems" on page 109*.

Step	Instructions
A	At the top, click **Objects > More object types > Network Object > Gateways and Servers > VSX > New Virtual System**.

Step	Instructions
B	On the **VSX System General Properties (Define the object name and the hosting VSX)** page: a. In the **Name** field, enter the applicable name for this object. In our example: `MyVs1` b. In the **VSX Gateway / Cluster** field, select the applicable VSX Gateway object. In our example: `MyVsxGw` c. Click **Next**.
C	On the **Virtual System Network Configuration (Define Virtual System Interfaces and Routes)** page: In our example, this Virtual System connects directly to two physical interfaces on the VSX Gateway. In the **Interfaces** section, add the "external" interface: a. Click **Add > Regular**. b. In the **Interface** field, select the applicable physical interface. In our example: `eth1` c. In the **IPv4 Configuration** section, enter the applicable **IP Address** and **Net Mask**. In our example: `192.168.10.1/24` You can select **Propagate route to adjacent Virtual Devices (IPv4)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv4 connectivity between neighboring Virtual Devices. d. In the **IPv6 Configuration** section, enter the applicable **IPv6 Address** and **Prefix**. You can select **Propagate route to adjacent Virtual Devices (IPv6)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv6 connectivity between the neighboring Virtual Devices. e. Click **OK**.

Step	Instructions
	In the **Interfaces** section, add the "internal" interface: a. Click **Add > Regular**. b. In the **Interface** field, select the applicable physical interface - this is the "internal" interface. In our example: `eth2` c. In the **IPv4 Configuration** section, enter the applicable **IP Address** and **Net Mask**. In our example: `172.30.10.1/24` You can select **Propagate route to adjacent Virtual Devices (IPv4)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv4 connectivity between the neighboring Virtual Devices. d. In the **IPv6 Configuration** section, enter the applicable **IPv6 Address** and **Prefix**. You can select **Propagate route to adjacent Virtual Devices (IPv6)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv6 connectivity between the neighboring Virtual Devices. e. Click **OK**. In the **Routes** section, click **Add** to configure the applicable static routes and the Default Route. Click **Next**.
D	On the **VSX System Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.
E	Examine the VSX configuration: a. Connect to the command line on the VSX Gateway. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

6. **Configure the first Virtual System object in SmartConsole**

See *"Working with Virtual Systems" on page 109*.

Step	Instructions
A	From the left navigation toolbar, click **Gateways & Servers**.
B	Open the first Virtual System object. In our example: `MyVs1`

Step	Instructions
C	Enable the applicable Software Blades. In our example: `IPsec VPN` blade 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 R82 Home Page.
D	Configure other applicable settings.
E	Click **OK** to push the updated VSX Configuration.
F	Configure and install the applicable policy on the first Virtual System object.
G	Examine the VSX configuration: a. Connect to the command line on the VSX Gateway. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

7. **Create the second Virtual System object in SmartConsole**

   See *"Working with Virtual Systems" on page 109*.

Step	Instructions
A	At the top, click **Objects > More object types > Network Object > Gateways and Servers > VSX > New Virtual System**.
B	On the **VSX System General Properties (Define the object name and the hosting VSX)** page: a. In the **Name** field, enter the applicable name for this object. In our example: `MyVs2` b. In the **VSX Gateway / Cluster** field, select the applicable VSX Gateway object. In our example: `MyVsxGw` c. Click **Next**.

Step	Instructions
C	On the **Virtual System Network Configuration (Define Virtual System Interfaces and Routes)** page: In our example, this Virtual System connects directly to two physical interfaces on the VSX Gateway. In the **Interfaces** section, add the "external" interface: a. Click **Add > Regular**. b. In the **Interface** field, select the applicable physical interface. In our example: `eth1` c. In the **IPv4 Configuration** section, enter the applicable **IP Address** and **Net Mask**. In our example: `192.168.20.1/24` You can select **Propagate route to adjacent Virtual Devices (IPv4)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv4 connectivity between Virtual Devices. d. In the **IPv6 Configuration** section, enter the applicable **IPv6 Address** and **Prefix**. You can select **Propagate route to adjacent Virtual Devices (IPv6)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv6 connectivity between Virtual Devices. e. Click **OK**.

Step	Instructions
	In the **Interfaces** section, add the "internal" interface: a. Click **Add > Regular**. b. In the **Interface** field, select the applicable physical interface - this is the "internal" interface. In our example: `eth2` c. In the **IPv4 Configuration** section, enter the applicable **IP Address** and **Net Mask**. In our example: `172.30.20.1/24` You can select **Propagate route to adjacent Virtual Devices (IPv4)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv4 connectivity between the neighboring Virtual Devices. d. In the **IPv6 Configuration** section, enter the applicable **IPv6 Address** and **Prefix**. You can select **Propagate route to adjacent Virtual Devices (IPv6)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv6 connectivity between the neighboring Virtual Devices. e. Click **OK**. In the **Routes** section, click **Add** to configure the applicable static routes and the Default Route. Click **Next**.
D	On the **VSX System Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.
E	Examine the VSX configuration: a. Connect to the command line on the VSX Gateway. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

8. **Configure the second Virtual System object in SmartConsole**

   See *"Working with Virtual Systems" on page 109*.

Step	Instructions
A	From the left navigation toolbar, click **Gateways & Servers**.
B	Open the second Virtual System object. In our example: `MyVs2`

Step	Instructions
C	Enable the applicable Software Blades. In our example: `Mobile Access` blade Refer to: ■ sk79700 - VSX supported features on R75.40VS and above ■ sk106496 - Software Blades updates on VSX R75.40VS and above - FAQ ■ Applicable *Administration Guide* on the R82 Home Page.
D	Configure other applicable settings.
E	Click **OK** to push the updated VSX Configuration.
F	Configure and install the applicable policy on the second Virtual System object.
G	Examine the VSX configuration: a. Connect to the command line on the VSX Gateway. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

Example 2: VSX Cluster managed by Multi-Domain Server

This example shows:

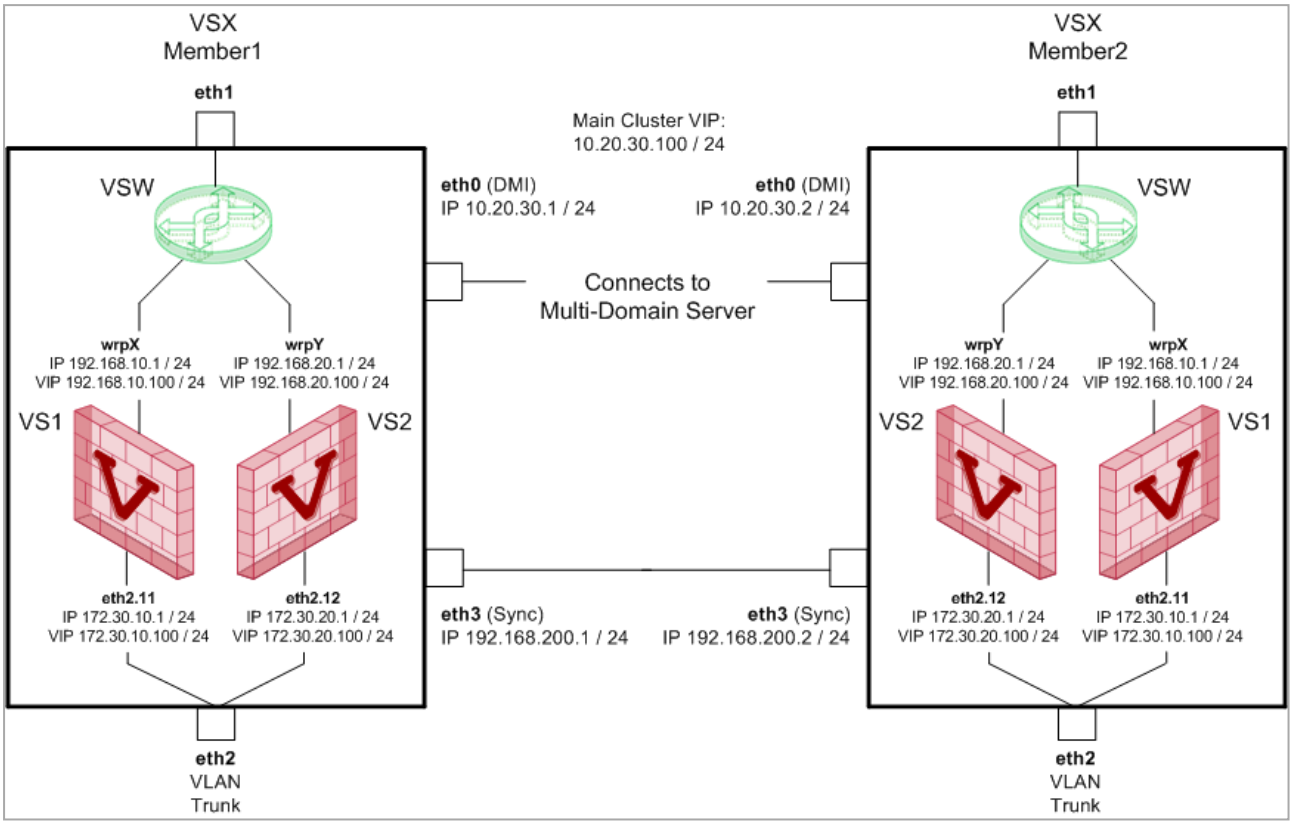
- One VSX Cluster in Virtual System Load Sharing (VSLS)
- Two VSX Cluster Members with DMI management connection
- One external Virtual Switch
- Two Virtual Systems:
  - External interface on each Virtual System connects directly to the Virtual Switch
  - Internal interface on each Virtual System connects to the VLAN Trunk interface
  - One Virtual System is configured with the IPsec VPN Software Blade
  - One Virtual System is configured with the Mobile Access Software Blade
- One Multi-Domain Server:
  - One Main Domain Management Server manages the objects of the VSX Cluster and Virtual Switch
  - One Target Domain Management Server manages the object of the first Virtual System
  - One Target Domain Management Server manages the object of the second Virtual System

Related documentation:

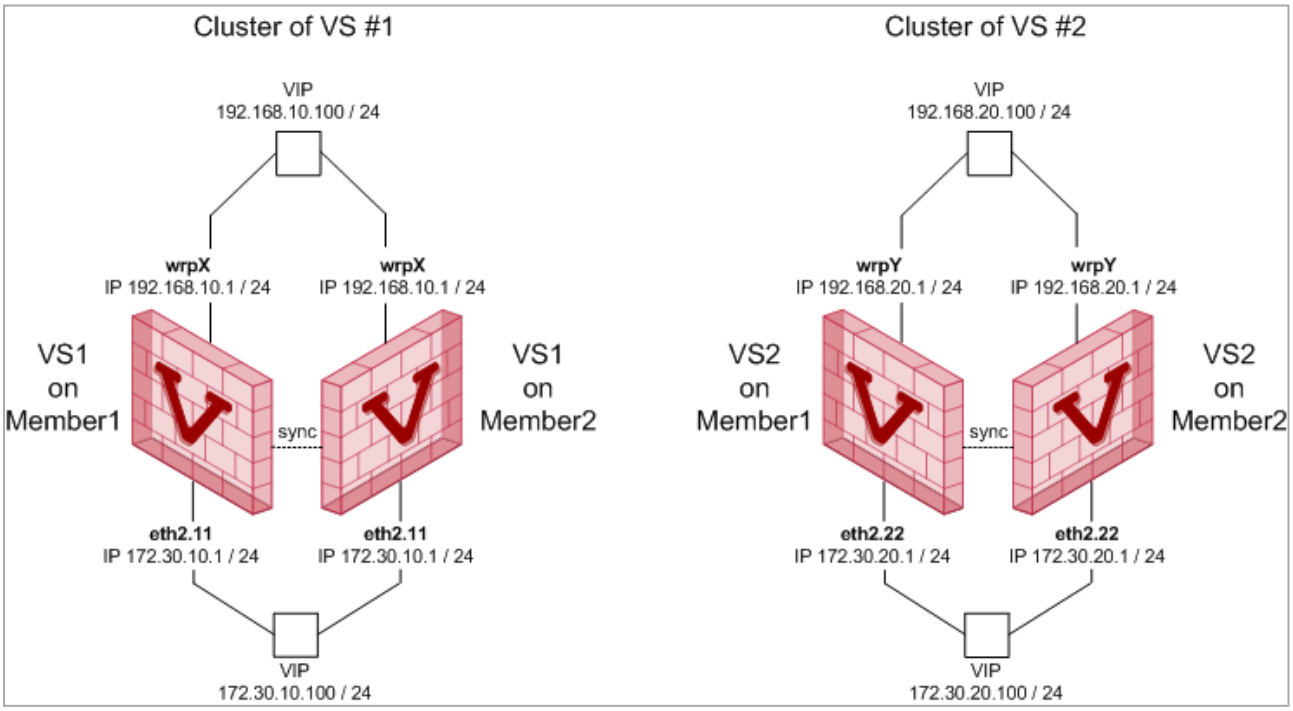
- *R82 Installation and Upgrade Guide*
- *R82 Gaia Administration Guide*
- *R82 Security Management Administration Guide*
- *R82 Multi-Domain Security Management Administration Guide*

Topology

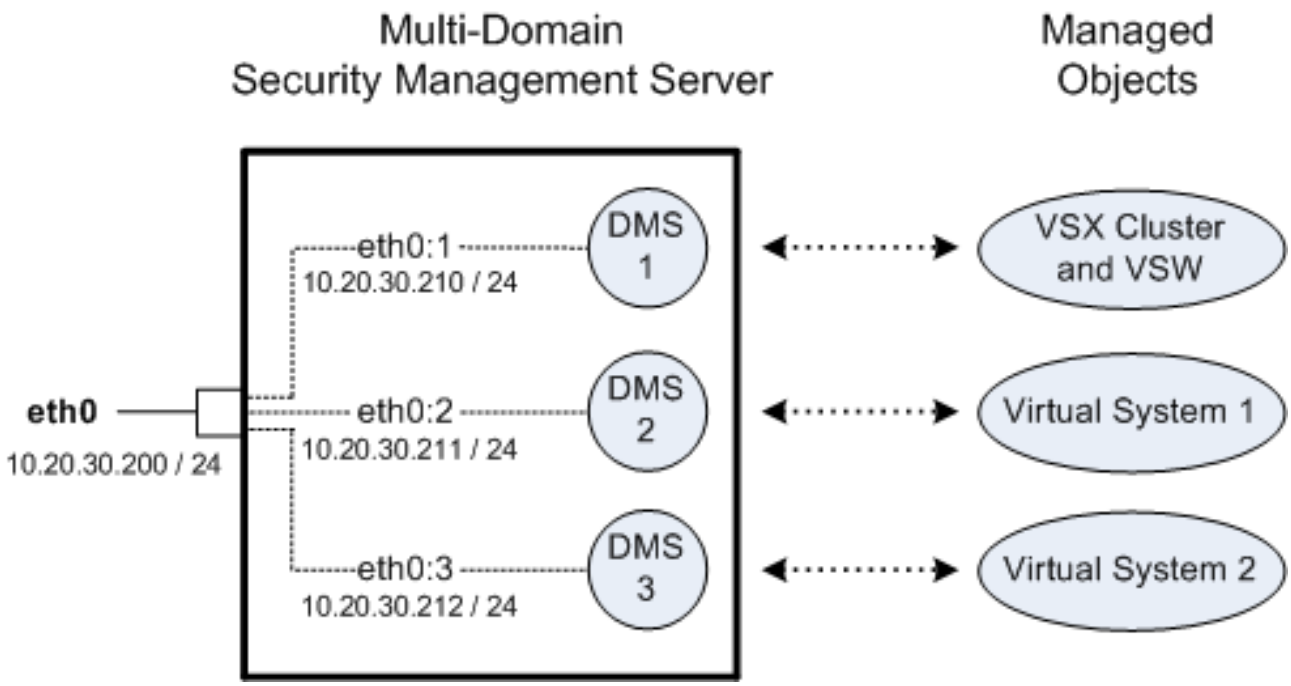
Topology of the VSX Cluster



Topology of the Virtual Systems in the cluster



Multi-Domain Server and managed objects



Interfaces and IP addresses

Computer	Interface	IP Address / Net Mask	Description
VSX Cluster Member 1	eth0	10.20.30.1/24 Main Cluster VIP 10.20.30.100/24	Dedicated Management Interface (DMI)
	eth1	none	External physical interface
	wrp*X*	192.168.10.1/24 Cluster VIP 192.168.10.100/24	External warp interface on Virtual System 1 Note - Interface name is generated automatically
	wrp*Y*	192.168.20.1/24 VIP 192.168.20.100/24	External warp interface on Virtual System 2 Note - Interface name is generated automatically
	eth2	none	Internal physical interface - VLAN Trunk
	eth2.11	172.30.10.1/24 Cluster VIP 172.30.10.100/24	Internal VLAN interface on Virtual System 1

Computer	Interface	IP Address / Net Mask	Description
	eth2.22	172.30.20.1/24 Cluster VIP 172.30.10.100/24	Internal VLAN interface on Virtual System 2
	eth3	192.168.200.1/24	Cluster Sync physical interface
VSX Cluster Member 2	eth0	10.20.30.2/24 Cluster VIP 10.20.30.100/24	Dedicated Management Interface (DMI)
	eth1	none	External physical interface
	wrp*X*	192.168.10.2/24 Cluster VIP 192.168.10.100/24	External warp interface on Virtual System 1 Note - Interface name is generated automatically
	wrp*Y*	192.168.20.2/24 Cluster VIP 192.168.20.100/24	External warp interface on Virtual System 2 Note - Interface name is generated automatically
	eth2	none	Internal physical interface - VLAN Trunk
	eth2.11	172.30.10.2/24 Cluster VIP 172.30.10.100/24	Internal VLAN interface on Virtual System 1
	eth2.22	172.30.10.2/24 Cluster VIP 172.30.10.100/24	Internal VLAN interface on Virtual System 2
	eth3	192.168.200.2/24	Cluster Sync physical interface
Multi-Domain Server	eth0	10.20.30.200/24	Leading Interface that belongs to the Multi-Domain Server
	eth0:1	10.20.30.210/24	Virtual interface that belongs to the Main Domain Management Server (DMS 1), which manages the VSX Cluster and Virtual Switch

Computer	Interface	IP Address / Net Mask	Description
	eth0:2	10.20.30.211/24	Virtual interface that belongs to the Target Domain Management Server (DMS 2), which manages the Virtual System 1
	eth0:3	10.20.30.212/24	Virtual interface that belongs to the Target Domain Management Server (DMS 3), which manages the Virtual System 2

Action Plan

1. **Install the Multi-Domain Server**

   See the *R82 Installation and Upgrade Guide*.

Step	Instructions
A	Install a Check Point appliance or Open Server.
B	Install Gaia OS.
C	Run the Gaia First Time Configuration Wizard. These settings are specific to the Multi-Domain Server: a. On the **Management Connection** page, select the applicable interface and configure the applicable IPv4 address. In our example: `eth0, 10.20.30.200/24` b. On the first **Installation Type** page, select **Multi-Domain Server**. c. On the second **Installation Type** page, select **Primary Multi-Domain Server**. d. On the **Leading VIP Interfaces Configuration** page, select the applicable interface. In our example: `eth0`
D	Install the applicable licenses.
E	Configure the applicable settings: a. Connect with SmartConsole to the Multi-Domain Server. b. Configure the applicable settings. c. Publish the SmartConsole session.

2. **Create the Main Domain Management Server in SmartConsole to manage the VSX Cluster and Virtual Switch**

Step	Instructions
A	Connect with SmartConsole to the Multi-Domain Server.
B	Create a new Domain and Domain Server. In our example: ■ Name: `DMS1` ■ IPv4: `10.20.30.210/24`
C	From the left navigation panel, click **Gateways & Servers**.
D	Configure the Main Domain Management Server: a. Connect with SmartConsole to the Main Domain Management Server (`DMS1`). b. Configure the applicable Management Software Blades and settings. c. Publish the SmartConsole session.

3. **Create the Target Domain Management Server in SmartConsole to manage the Virtual System 1**

Step	Instructions
A	Connect with SmartConsole to the Multi-Domain Server.
B	Create a new Domain and Domain Server. In our example: ■ Name: `DMS2` ■ IPv4: `10.20.30.211/24`
C	From the left navigation panel, click **Gateways & Servers**.
D	Configure the Target Domain Management Server: a. Connect with SmartConsole to the Target Domain Management Server (`DMS2`). b. Configure the applicable Management Software Blades and settings. c. Publish the SmartConsole session.

4. **Create the Target Domain Management Server in SmartConsole to manage the Virtual System 2**

Step	Instructions
A	Connect with SmartConsole to the Multi-Domain Server.
B	Create a new Domain and Domain Server. In our example: ■ Name: `DMS3` ■ IPv4: `10.20.30.212/24`
C	From the left navigation panel, click **Gateways & Servers**.
D	Configure the Target Domain Management Server: a. Connect with SmartConsole to the Target Domain Management Server (`DMS3`). b. Configure the applicable Management Software Blades and settings. c. Publish the SmartConsole session.

5. **Install the VSX Cluster Member 1**

   See the *R82 Installation and Upgrade Guide*.

Step	Instructions
A	Install a Check Point appliance or Open Server.
B	Make sure you have enough physical interfaces for your VSX topology.
C	Install Gaia OS.
D	Run the Gaia First Time Configuration Wizard. These settings are specific to the VSX Cluster Member 1: a. On the **Management Connection** page, select the interface for the DMI management connection and configure the applicable IPv4 address. In our example: `eth0, 10.20.30.1/24` b. On the **Internet Connection** page, do **not** configure IP addresses on physical interfaces, to which your Virtual Systems connect directly. c. On the **Installation Type** page, select **Security Gateway and/or Security Management**. d. On the **Products** page, select **Security Gateway**. e. On the **Dynamically Assigned IP** page, select **No**.

Step	Instructions
E	Make sure to enable the applicable physical interfaces: To enable a physical interface in Gaia Portal a. Connect to the Gaia Portal in your web browser. In our example: `https://10.20.30.1` b. Click **Network Management > Network Interfaces**. c. In the upper left corner, click the lock icon to obtain the configuration lock. d. Select the applicable physical interface > click **Edit**. e. Select **Enable**. f. Click **OK**. To enable a physical interface in Gaia Clish, run: a. `set interface <Name of Physical Interface> state on` b. `save config`
F	Install the applicable licenses.
G	Enable the **Per Virtual System State** mode: a. Connect to the command line. b. Log in to Gaia Clish, or Expert mode. c. Run: `cpconfig` d. Select: **Enable Check Point Per Virtual System State** e. Enter **y** to confirm f. Run: `reboot`

6. **Install the VSX Cluster Member 2**

   See the *R82 Installation and Upgrade Guide*.

Step	Instructions
A	Install a Check Point appliance or Open Server.
B	Make sure you have enough physical interfaces for your VSX topology.
C	Install Gaia OS.

Step	Instructions
D	Run the Gaia First Time Configuration Wizard. These settings are specific to the VSX Cluster Member 1: a. On the **Management Connection** page, select the interface for the DMI management connection and configure the applicable IPv4 address. In our example: `eth0, 10.20.30.2/24` b. On the **Internet Connection** page, do **not** configure IP addresses on physical interfaces, to which your Virtual Systems connect directly. c. On the **Installation Type** page, select **Security Gateway and/or Security Management**. d. On the **Products** page, select **Security Gateway**. e. On the **Dynamically Assigned IP** page, select **No**.
E	Make sure to enable the applicable physical interfaces: To enable a physical interface in Gaia Portal a. Connect to the Gaia Portal in your web browser. In our example: `https://10.20.30.2` b. Click **Network Management > Network Interfaces**. c. In the upper left corner, click the lock icon to obtain the configuration lock. d. Select the applicable physical interface > click **Edit**. e. Select **Enable**. f. Click **OK**. To enable a physical interface in Gaia Clish, run: a. `set interface <Name of Physical Interface> state on` b. `save config`
F	Install the applicable licenses.
G	Enable the **Per Virtual System State** mode: a. Connect to the command line. b. Log in to Gaia Clish, or Expert mode. c. Run: `cpconfig` d. Select: **Enable Check Point Per Virtual System State** e. Enter **y** to confirm f. Run: `reboot`

7. **Create the VSX Cluster object with VSX Cluster Members in SmartConsole**

See *"Configuring VSX Clusters" on page 185* and *"Working with VSX Clusters" on page 191*.

Step	Instructions
A	Connect with SmartConsole to the Main Domain Management Server that manages the objects of the VSX Cluster and Virtual Switch. In our example: `DMS1`
B	At the top, click **Objects > More object types > Network Object > Gateways and Servers > VSX > New Cluster**.
C	On the **VSX Cluster General Properties (Specify the object's basic settings)** page: a. In the **Enter the VSX Cluster Name** field, enter the applicable name for this object. In our example: `MyVsxCluster` b. In the **Enter the VSX Cluster IPv4** field, enter the Cluster Virtual IPv4 address that is configured on the Dedicated Management Interfaces (DMI). In our example: `10.20.30.100` c. In the **Enter the VSX Cluster IPv6** field, enter the Cluster Virtual IPv6 address that is configured on the Dedicated Management Interfaces (DMI). d. In the **Select the VSX Cluster Version** field, select the applicable Check Point version. In our example: `R82` e. In the **Select the VSX Cluster Platform** field, select **ClusterXL Virtual System Load Sharing**. See *"Configuring Virtual System Load Sharing (VSLS)" on page 213*. **Note** - This is the only mode available for a VSX Cluster that was installed as R81.10 or higher. f. Click **Next**.

Step	Instructions
D	On the **VSX Cluster Members (Define the members of this VSX Cluster)** page: Add the first VSX Cluster Member: a. Click **Add**. b. In the **Cluster Member Name** field, enter the applicable name for this object. In our example: `MyVsxMember1` c. In the **Cluster Member IPv4 Address** field, enter the IPv4 address of the Dedicated Management Interface (DMI). In our example: `eth0`, `10.20.30.1` d. In the **Enter the VSX Gateway IPv6** field, enter the applicable IPv6 address. e. In the **Activation Key** field, enter the same Activation Key you entered during the First Time Configuration Wizard of this VSX Cluster Member. f. In the **Confirm Activation Key** field, enter the same Activation Key again. g. Click **Initialize**. h. Click **OK**. i. Enter the same Activation Key you entered in the `cpconfig` menu. j. Click **Initialize**.
	If the **Trust State** field does not show **Trust established**, perform these steps: a. Connect to the command line on the VSX Cluster Member. b. Make sure there is a physical connectivity between the VSX Cluster Member 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. On the **VSX Cluster General Properties** page, click **Reset**. g. Enter the same Activation Key you entered in the `cpconfig` menu. h. Click **Initialize**.

Step	Instructions
E	On the **VSX Cluster Members (Define the members of this VSX Cluster)** page: Add the second VSX Cluster Member: a. Click **Add**. b. In the **Cluster Member Name** field, enter the applicable name for this object. In our example: `MyVsxMember2` c. In the **Cluster Member IPv4 Address** field, enter the IPv4 address of the Dedicated Management Interface (DMI). In our example: `eth0`, `10.20.30.2` d. In the **Enter the VSX Gateway IPv6** field, enter the applicable IPv6 address. e. In the **Activation Key** field, enter the same Activation Key you entered during the First Time Configuration Wizard of this VSX Cluster Member. f. In the **Confirm Activation Key** field, enter the same Activation Key again. g. Click **Initialize**. h. Click **OK**. i. Click **Next**.
	If the **Trust State** field does not show **Trust established**, perform these steps: a. Connect to the command line on the VSX Cluster Member. b. Make sure there is a physical connectivity between the VSX Cluster Member 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. On the **VSX Cluster General Properties** page, click **Reset**. g. Enter the same Activation Key you entered in the `cpconfig` menu. h. Click **Initialize**.

Step	Instructions
F	On the **VSX Cluster Interfaces (Physical Interfaces Usage)** page: a. Examine the list of the interfaces - it must show all the physical interfaces on the VSX Gateway. b. If you plan to connect more than one Virtual System directly to same physical interface, you must select **VLAN Trunk** for that physical interface. In our example: `eth2` c. Click **Next**.

G	On the **VSX Cluster members (Synchronization Network)** page:
	a. Select the interface that will be used for state synchronization.
	In our example: `eth3`
	b. Configure the IPv4 addresses for the Sync interfaces on each VSX Cluster Member.
	In our example:
	`MyVsxMember1 - 192.168.200.1 / 255.255.255.0`
	`MyVsxMember2 - 192.168.200.2 / 255.255.255.0`
	c. Click **Next**.

H	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 Network Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router. b. Click **Next**.
I	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.
J	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
K	Examine the VSX configuration: a. Connect to the command line on each VSX Cluster Member. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

8. **Configure the VSX Cluster object in SmartConsole**

See *"Working with VSX Clusters" on page 191*.

Step	Instructions
A	From the left navigation toolbar, click **Gateways & Servers**.
B	Open the VSX Cluster object. In our example: `MyVsxCluster`
C	Enable the applicable Software Blades. 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 R82 Home Page.
D	Configure other applicable settings.
E	Click **OK** to push the updated VSX Configuration. Click **View Report** for more information.
F	Install policy on the VSX Cluster object: a. Click **Install Policy**. b. In the **Policy** field, select the default policy for this VSX Cluster object. This policy is called: `<Name of VSX Cluster object>_VSX`. In our example: `MyVsxCluster_VSX` c. Click **Install**.
G	Examine the VSX configuration and VSX Cluster configuration: a. Connect to the command line on each VSX Cluster Member. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v` d. Run: ■ In Gaia Clish: `show cluster state` ■ In the Expert mode: `cphaprob state`

9. **Create the Virtual Switch object in SmartConsole**

Step	Instructions
A	Connect with SmartConsole to the Main Domain Management Server that manages the objects of the VSX Cluster and Virtual Switch. In our example: `DMS1`
B	Create the Virtual Switch object: At the top, click **Objects > More object types > Network Object > Gateways and Servers > VSX > New Virtual Switch**.
C	On the **VSX Switch General Properties (Define the object name and the hosting VSX)** page: a. In the **Name** field, enter the applicable name for this object. In our example: `MyVsw` b. In the **VSX Gateway / Cluster** field, select the applicable VSX Gateway or VSX Cluster object. In our example: `MyVsxCluster` c. Click **Next**.
D	On the **VSX Switch Network Configuration (Define Virtual Switch Interfaces)** page: a. Click **Add**. b. In the Interface field, select the applicable physical interface. In our example: `eth2` c. Click **OK**. d. Click **Next**.
E	On the **VSX Switch Cluster Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.
F	Examine the VSX configuration: a. Connect to the command line on each VSX Cluster Member. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

10. **Create the first Virtual System object in SmartConsole**

Step	Instructions
A	Connect with SmartConsole to the Target Domain Management Server that manages the object of the first Virtual System. In our example: `DMS2`

Step	Instructions
B	In SmartConsole, create the first Virtual System object: See *"Working with Virtual Systems" on page 109*. At the top, click **Objects > More object types > Network Object > Gateways and Servers > VSX > New Virtual System**.
C	On the **VSX System General Properties (Define the object name and the hosting VSX)** page: a. In the **Name** field, enter the applicable name for this object. In our example: `MyVs1` b. In the **VSX Gateway / Cluster** field, select the applicable VSX Gateway or VSX Cluster object. In our example: `MyVsxCluster` c. Click **Next**.
D	On the **Virtual System Network Configuration (Define Virtual System Interfaces and Routes)** page: In our example, this Virtual System connects to the Virtual Switch ("external") and to the physical VLAN Trunk interface ("internal") on the VSX Cluster Members. In the **Interfaces** section, add the "external" interface: a. Click **Add > Leads to Virtual Switch**. **Add Interface** window opens. b. In the **Leads to** field, select the Virtual Switch your created earlier. In our example: `MyVsxVsw` c. In the **IPv4 Configuration** section, enter the applicable **IP Address** and **Net Mask**. In our example: `192.168.10.1/24` d. In the **IPv6 Configuration** section, enter the applicable **IPv6 Address** and **Prefix**. e. Click **OK**.

Step	Instructions
	In the **Interfaces** section, add the "internal" interface: a. Click **Add > Regular**. b. In the **Interface** field, select the applicable physical interface - this is the "internal" interface. In our example: `eth2` (that is marked as VLAN Trunk) c. In the **VLAN tag** field, enter the applicable number between 2 and 4094. In our example: `11` (to configure `eth2.11`) d. In the **IPv4 Configuration** section, enter the applicable **IP Address** and **Net Mask**. In our example: `172.30.10.1/24` You can select **Propagate route to adjacent Virtual Devices (IPv4)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv4 connectivity between the neighboring Virtual Devices. e. In the **IPv6 Configuration** section, enter the applicable **IPv6 Address** and **Prefix**. You can select **Propagate route to adjacent Virtual Devices (IPv6)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv6 connectivity between the neighboring Virtual Devices. f. Click **OK**. In the **Routes** section, click **Add** to configure the applicable static routes and the Default Route. Click **Next**.
E	On the **Virtual System Cluster Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.
F	Examine the VSX configuration: a. Connect to the command line on each VSX Cluster Member. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

11. **Configure the first Virtual System object in SmartConsole**

    See *"Working with Virtual Systems" on page 109*.

Step	Instructions
A	From the left navigation toolbar, click **Gateways & Servers**.
B	Open the first Virtual System object. In our example: `MyVs1`
C	Enable the applicable Software Blades. In our example: `IPsec VPN` blade 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 R82 Home Page.
D	Configure other applicable settings.
E	Click **OK** to push the updated VSX Configuration.
F	Configure and install the applicable policy on the first Virtual System object.
G	Examine the VSX configuration and VSX Cluster configuration: a. Connect to the command line on each VSX Cluster Member. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v` d. Run: ■ In Gaia Clish: `show cluster state` ■ In the Expert mode: `cphaprob state`

12. **Create the second Virtual System object in SmartConsole**

Step	Instructions
A	Connect with SmartConsole to the Target Domain Management Server that manages the object of the first Virtual System. In our example: `DMS3`
B	In SmartConsole, create the first Virtual System object: See *"Working with Virtual Systems" on page 109*. At the top, click **Objects > More object types > Network Object > Gateways and Servers > VSX > New Virtual System**.

Step	Instructions
C	On the **VSX System General Properties (Define the object name and the hosting VSX)** page: a. In the **Name** field, enter the applicable name for this object. In our example: `MyVs2` b. In the **VSX Gateway / Cluster** field, select the applicable VSX Gateway or VSX Cluster object. In our example: `MyVsxCluster` c. Click **Next**.
D	On the **Virtual System Network Configuration (Define Virtual System Interfaces and Routes)** page: In our example, this Virtual System connects to the Virtual Switch ("external") and to the physical VLAN Trunk interface ("internal") on the VSX Cluster Members. In the **Interfaces** section, add the "external" interface: a. Click **Add > Leads to Virtual Switch**. b. In the **Leads to** field, select the Virtual Switch your created earlier. In our example: `MyVsxVsw` c. In the **IPv4 Configuration** section, enter the applicable **IP Address** and **Net Mask**. In our example: `192.168.20.1/24` d. In the **IPv6 Configuration** section, enter the applicable **IPv6 Address** and **Prefix**. e. Click **OK**.

Step	Instructions
	In the **Interfaces** section, add the "internal" interface: a. Click **Add > Regular**. b. In the **Interface** field, select the applicable physical interface - this is the "internal" interface. In our example: `eth2` (that is marked as VLAN Trunk) c. In the **VLAN tag** field, enter the applicable number between 2 and 4094. In our example: `22` (to configure `eth2.22`) d. In the **IPv4 Configuration** section, enter the applicable **IP Address** and **Net Mask**. In our example: `172.30.20.1/24` You can select **Propagate route to adjacent Virtual Devices (IPv4)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv4 connectivity between the neighboring Virtual Devices. e. In the **IPv6 Configuration** section, enter the applicable **IPv6 Address** and **Prefix**. You can select **Propagate route to adjacent Virtual Devices (IPv6)** to "advertise" this Virtual System to neighboring Virtual Devices. This enables IPv6 connectivity between the neighboring Virtual Devices. f. Click **OK**. In the **Routes** section, click **Add** to configure the applicable static routes and the Default Route. Click **Next**.
E	On the **Virtual System Cluster Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.
F	Examine the VSX configuration: a. Connect to the command line on each VSX Cluster Member. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v`

13. **Configure the second Virtual System object in SmartConsole**

See *"Working with Virtual Systems" on page 109*.

Step	Instructions
A	From the left navigation toolbar, click **Gateways & Servers**.
B	Open the second Virtual System object. In our example: `MyVs2`
C	Enable the applicable Software Blades. In our example: `Mobile Access` blade 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 R82 Home Page.
D	Configure other applicable settings.
E	Click **OK** to push the updated VSX Configuration.
F	Configure and install the applicable policy on the second Virtual System object.
G	Examine the VSX configuration and VSX Cluster configuration: a. Connect to the command line on each VSX Cluster Member. b. Log in to Gaia Clish, or Expert mode. c. Run: `vsx stat -v` d. Run: ■ In Gaia Clish: `show cluster state` ■ In the Expert mode: `cphaprob state`

Working with Kernel Parameters

See the *R82 Quantum Security Gateway Guide* > Chapter "Working with Kernel Parameters".

Kernel Debug on Security Gateway

See the *R82 Quantum Security Gateway Guide* > Chapter "Kernel Debug on Security Gateway".

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

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. 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 Distributor. 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.

D

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 a DHCP server, by an 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.

Dedicated Management Interface
Separate physical interface on Traditional VSX Gateway or Traditional VSX Cluster Members, through which Check Point Security Management Server or Multi-Domain Security Management Server connects directly to Traditional VSX Gateway or Traditional VSX Cluster Members. DMI is restricted to management traffic, such as provisioning, logging and monitoring. Acronym: DMI.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

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 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 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.

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

Main Domain Management Server
Domain Management Server on a Multi-Domain Security Management Server, on which you configured the object of your Traditional VSX Gateway or Traditional VSX Cluster. In this case, objects of your Virtual Systems are defined on different Domain Management Servers (Target Domain Management Servers).

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 Security Management 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.

Non-Dedicated Management Interface
Shared physical interface on Traditional VSX Gateway or Traditional VSX Cluster Members (supported only in versions R80.40 and lower), which carries user "production" traffic and through which Check Point Security Management Server or Multi-Domain Security Management Server connects to Traditional VSX Gateway or Traditional VSX Cluster Members. Non-DMI configuration requires the use of a Virtual Router or Virtual Switch. Acronym: Non-DMI.

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 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.

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.

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.

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.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Target Domain Management Server
Domain Management Server on a Multi-Domain Security Management Server, on which you configured the objects of your Virtual Systems. In this case, object of your Traditional VSX Gateway or Traditional VSX Cluster are defined on a different Domain Management Server (Main Domain Management Server).

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.

Traditional VSX Gateway
Physical server that hosts Traditional 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.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

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

Virtual Device
Logical object that emulates the functionality of a type of physical network object. Virtual Device can be on of these: Virtual Router, Virtual System, or Virtual Switch.

Virtual Router
Virtual Device on a Traditional VSX Gateway or Traditional VSX Cluster Member that functions as a physical router. Acronym: VR.

Virtual Switch
Virtual Device on a Traditional VSX Gateway or Traditional VSX Cluster Member that functions as a physical switch. Acronym: VSW.

Virtual System
Virtual Device on a Traditional VSX Gateway or Traditional VSX Cluster Member that implements the functionality of a Security Gateway. Acronym: VS.

Virtual System Load Sharing
Traditional VSX Cluster technology that assigns Virtual System traffic to different Active Cluster Members. Acronym: VSLS.

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.

W

Warp Jump
If two Virtual Systems connect to the same Virtual Switch or Virtual Router, then internally traffic that must pass from a network behind one Virtual System to a network behind another Virtual System, "jumps" from one Virtual System to another Virtual System without passing through the Virtual Switch or Virtual Router.

Warp Link
Logical interface that is created automatically: (1) In a VSNext topology, between a Virtual Gateway and a Virtual Switch (2) In a Traditional VSX topology, between a Virtual System and a Virtual Switch (3) In a Traditional VSX topology, between a Virtual System and a Virtual Router. Acronym: WRP.

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.