How to Work with Layer 2 VS in VSX
Objective

This document explains how to create a Layer-2 Virtual Switch and Virtual System in Bridge Mode in a VSX Environment. It shows common configuration options.

Make sure you have the latest version of this document.

Details

Supported Versions

- VSX NGX R65
- VSX NGX R67.X
- R75.40VS
- R76
- R77, R77.10 and R77.20

Supported OS

- SecurePlatform
- GAiA
- IPSO

Supported Appliances

- Appliances that support the above versions and Operating Systems

Before You Start

Related Documentation and Assumed Knowledge

- VSX NGX R65 Administration Guide
- VSX NGX R67 Administration Guide
- R75.40VS VSX Administration Guide
- R76 VSX Administration Guide
- R77 VSX Administration Guide

Impact on the Environment and Warnings

If you change your VSX Network topology, communication can be lost between your Virtual Systems and resources (external and internal). Make sure changes you make do not conflict with current network configurations.
When to use a Virtual System in Bridge Mode or a Virtual Switch

A Virtual System in Bridge Mode implements native layer-2 bridging. With this implementation you can insert another inspection point without segmenting the existing virtual network. 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.

A Virtual Switch is a software abstraction of a physical Ethernet switch that can connect to physical switches through physical network adapters. This allows the Virtual network to join with the physical networks. The Virtual Switch connects Virtual Systems and facilitates sharing a common physical interface without segmenting the existing network.

When sharing a physical interface through a Virtual Switch, there is no need to allocate an additional subnet for IP Addresses of a Virtual System connected to the switch. There is no need to manually configure the routing on the routers adjacent to the shared interface. Similar to a physical switch, the Virtual Switch maintains a forwarding table with a list of MAC Addresses and their associated ports.

Creating a Virtual Switch and a Virtual System in Bridge Mode

To create a Virtual Switch:
1. Open SmartDashboard to your Security Management Server or Domain Management Server.
2. In Network Objects, right-click Check Point, and select VSX > Virtual Switch.
3. Enter a name and select the VSX Gateway or Cluster that this switch will be added to, and click Next.
4. In the next step, click Add.
5. Enter the name of the interface for the Virtual Switch. Click Next.
6. Click Finish to complete the Wizard.

Creating a Virtual System in Bridge Mode
1. Open SmartDashboard to your Management Station or Domain Management System.
2. In Network Objects, right-click Check Point, and select VSX > Virtual System.
   The Virtual System wizard opens.
3. Enter a name for the Virtual System.
4. Select the VSX Gateway or Cluster that this Virtual System will belong to.
5. Select Bridge Mode.
   If you want, you can override the Creation Template and create a Custom Virtual System.
6. Click Next.
7. Add the required interfaces to your Virtual System. Click Next.
8. Click **Finish**.

## Completing the Procedure

When you click Finish in the wizard, the Virtual Switch or Virtual System is created on the hosting VSX Gateway or Cluster.

To see or change the properties of the new Network Object, double-click it, in the SmartDashboard of the server that manages the hosting VSX Gateway or Cluster.

## Verifying

To make sure of connectivity in the Virtual Network, test connectivity between all Virtual Systems, Virtual Switches and Virtual Routers on the VSX Gateway/Cluster.

From the CLI, run these commands to see data about the Virtual Switch or Virtual System in Bridge Mode that you created.

### Display VSX Status

From the Expert shell, run this command to see details of all virtual devices on the VSX Gateway/Cluster.

**Syntax:** `vsx stat -l [-v]`

**Note:** `--v = verbose output`
Example: `vsx stat -l`

```
[Expert@GAIAR77USX:~]# vsx stat -l

USID: 0
URID: 0
Type: USX Gateway
Name: GAIAR77USX
Security Policy: Standard
Installed at: 15Nov2014 1:24:03
SIC Status: Trust
Connections number: 1
Connections peak: 61
Connections limit: 14900

USID: 1
URID: 1
Type: Virtual System in Bridge mode
Name: Pre-Internal
Security Policy: Standard
Installed at: 15Nov2014 1:24:05
SIC Status: Trust
Connections number: 0
Connections peak: 10
Connections limit: 14900
```

Example: `vsx stat -l -v`

```
[Expert@GAIAR77USX:~]# vsx stat -l -v

USX Gateway Status

Name: GAIAR77USX
Security Policy: Standard
Installed at: 15Nov2014 1:24:03
SIC Status: Trust

Number of Virtual Systems allowed by license: 0
Virtual Systems [active / configured]: 1 / 1
Virtual Routers and Switches [active / configured]: 0 / 0
Total connections [current / limit]: 2 / 29800

Virtual Devices Status

<table>
<thead>
<tr>
<th>ID</th>
<th>Type &amp; Name</th>
<th>Security Policy</th>
<th>Installed at</th>
<th>SIC Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Pre-Internal</td>
<td>Standard</td>
<td>15Nov2014 1:24:03</td>
<td>Trust</td>
</tr>
</tbody>
</table>

Type: S - Virtual System, B - Virtual System in Bridge mode, R - Virtual Router, W - Virtual Switch.
```

Note - For Virtual Switches, the Security Policy Field will be empty.
Troubleshooting

If you suspect that a Virtual System is experiencing connectivity issues:

1. **Run:** `vsenv`
   This sets the context to the appropriate Virtual System.

2. **Run:** `fw getifs`
   This shows the interface list for the Virtual System.

3. **Look at the connectivity status with standard operating system commands**, such as: `ping, traceroute, tcpdump, ip route, ftp, etc`. Some of these run according to context (for example, routing, source and destination IP addresses). You can also run the `ip route` and `ip link` commands.

If these tests show that all interfaces and routers have connectivity, and appear to be functioning correctly, monitor the passage of packets through the system.

**Run:** `fw monitor -v <vsid>`

This captures 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.

**Note** - Performance Pack can have an adverse effect on the capabilities of the `fw monitor` command.

**Run:** `tcpdump`

This shows transmitted or received packets for specific interfaces, including Warp interfaces. This often gives valuable clues for resolving connectivity issues.