In This Document

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Unified Graphical User Interface</td>
<td>2</td>
</tr>
<tr>
<td>Single IP for Management</td>
<td>2</td>
</tr>
<tr>
<td>Virtual System Creation wizard</td>
<td>2</td>
</tr>
<tr>
<td>Virtual System Creation Templates</td>
<td>3</td>
</tr>
<tr>
<td>Easier Connection to Authentication Servers</td>
<td>3</td>
</tr>
<tr>
<td>Virtual Switch</td>
<td>4</td>
</tr>
<tr>
<td>Virtual System in Bridge Mode</td>
<td>4</td>
</tr>
<tr>
<td>Unnumbered Interface Support</td>
<td>4</td>
</tr>
<tr>
<td>Increased number of interfaces</td>
<td>5</td>
</tr>
<tr>
<td>Increased number of interfaces</td>
<td>5</td>
</tr>
<tr>
<td>Dynamic Routing Support</td>
<td>5</td>
</tr>
<tr>
<td>Backward Compatibility Support</td>
<td>5</td>
</tr>
<tr>
<td>Clustering Enhancements</td>
<td>5</td>
</tr>
<tr>
<td>Routing Enhancements</td>
<td>6</td>
</tr>
<tr>
<td>Enhancements to SmartDefense</td>
<td>7</td>
</tr>
<tr>
<td>Licensing</td>
<td>7</td>
</tr>
<tr>
<td>NAT Enhancements</td>
<td>7</td>
</tr>
<tr>
<td>SecurePlatform Add-Ons &amp; Enhancements</td>
<td>8</td>
</tr>
<tr>
<td>New monitoring classes for Status Information</td>
<td>10</td>
</tr>
</tbody>
</table>

The latest version of the “What’s New” documentation is available for download from:
http://www.checkpoint.com/techsupport/downloads.jsp
Introduction

This document covers the new capabilities of VPN-1 VSX NGX.

Unified Graphical User Interface

All VSX provisioning and maintenance operations are performed through SmartDashboard.

Single IP for Management

In previous versions (VSX 2.0.1, VSX NG AI) the VSX installation process created a default Virtual System called the Management Virtual System (MVS). Instead of the MVS, the VSX gateway object now:

- Handles provisioning and configuration of Virtual Systems and Virtual Routers.
- Manages Gateway State Synchronization when working with clusters.
- Provides a single IP for communication with the management entity (Provider-1, SmartCenter, LDAP Server, Radius, TACACS, SNMP). All management communication between the VSX gateway and management entity takes place via single IP address. The TCP connection is terminated at the VSX gateway, and does not continue to the Virtual Device. In a cluster environment, each cluster is managed by a single IP address. Members of the cluster are automatically assigned IP addresses.

Single IP for Cluster Management

In a VSX cluster, only the cluster members require an IP address. This reduces the overall number of IP addresses required to manage the cluster. For example, a VSX system with one hundred Virtual Systems on four cluster members requires only four IP addresses for management, one for each cluster member. The Virtual systems within any cluster member are managed by internally assigned IP addresses.

Virtual System Creation wizard

A new wizard simplifies the creation of Virtual Systems.
Virtual System Creation Templates

Virtual Systems can be created with a predefined networking configuration for use in the most common VSX deployments. During the creation of a VSX gateway, a Virtual System creation template page appears:

This page provides two networking templates for Virtual Systems:

- All Virtual Systems have their own internal interface but share a single external interface
- Each Virtual System has its own external and internal interfaces

The third alternative is not to use one of the templates, but customize each Virtual System according to your VSX deployment.

Choice of Management Models

The choice of Virtual System creation template also decides the management model for the VSX deployment: whether or not there will be an interface dedicated to the management of the VSX system.

Easier Connection to Authentication Servers

In versions previous to VSX NGX, the warp cable (wrp5000) provided a direct link between Virtual Systems and the MVS (the Virtual System reserved for management) which was then used for connecting with external authentication servers such as LDAP, RADIUS, TACACS, and TACACS+. In NGX, there are two options available for enabling connectivity between Virtual Systems and external authentication servers:

- Shared
- Private
When the shared option is configured, authentication servers are accessible by all Virtual Systems via the VSX gateway. When the private option is configured, authentication servers are accessed directly by the Virtual System.

Virtual Switch

In versions previous to VSX NGX, the only way to share an interface between multiple Virtual Systems, or to connect between Virtual Systems, was through a Virtual Router. The new Virtual Switch connects between Virtual Systems, and facilitates the sharing of a physical interface without segmenting the existing IP network.

A Virtual Switch provides layer 2 connectivity between Virtual Systems and connectivity to a shared interface. As with a physical switch, each Virtual Switch maintains a forwarding table with a list of MAC addresses and their associated ports. The forwarding decision is made by inspecting the MAC destination address of each incoming packet.

When sharing a physical interface through 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.

Virtual System in Bridge Mode

By providing a Virtual System that implements native layer-2 bridging instead of IP routing, a VSX gateway provides transparent security inspection.

A typical network connection in such a scenario will involve a 802.1q VLAN switch on either side of the VSX gateway. The interfaces of the bridge do not require IP addresses. The Virtual System in bridge mode remain transparent to the existing IP network.

A Virtual System in Bridge mode:
- Has the same Firewall security capabilities of a Virtual System except for VPN and NAT (NAT modifies layer-3 information)
- Enables easier configuration of Virtual Systems since no IP addresses or specific routing information is required.
- Does not segment an existing network.

Unnumbered Interface Support

To reduce the amount of IP addresses required in a VSX deployment, Virtual Systems within a VSX gateway now support unnumbered interfaces. This is possible where the interface on the Virtual System is connected to a Virtual Router, and Hide NAT or VPN features are not enabled.
**Increased number of interfaces**

Each Virtual System now supports up to sixty-four separate interfaces.

**Dynamic Routing Support**

Dynamic Routing (DR) is now performed locally on the gateway. A context aware CLI command “\texttt{vrf - connect}” is available which determines to which Virtual System or Virtual Router the dynamic routing applies. Supported dynamic protocols:

**Unicast:**
- OSPF
- RIP
- BGP

**Multicast:**
- IGMP
- PIM-SM
- PIM-DM

**Backward Compatibility Support**

Full backward compatibility. From the current NGX release, you create and manage VSX 2.0.1 and VSX\_NG\_AI objects.

**Clustering Enhancements**

**Adding New Members to a Cluster**

Adding/removing members from a cluster. In versions previous to VSX NGX, you could not add or remove members from an existing cluster. In NGX, using the command line \texttt{VSX\_Utility} tool, new members can be added or removed from an existing cluster.

**Upgrading Cluster Members**

The \texttt{VSX\_Utility} tool is also used to upgrade members of a cluster. Once the member module has been upgraded, the configuration of the (pre-upgrade) module, contained in the Management server database, is pushed back to the new (upgraded) module.
**VSX Gateway Recovery**

The `vsx_util` command line is also used to recover fallen modules. For example, after a hard disk failure. Once the hard disk has been replaced, a new module installed, and SIC established with the management server, the `vsx_util` command returns the modules previous configuration (stored in the management database) to the module.

**Single Virtual System failover**

In a clusterXL environment, Virtual Systems running in bridge mode are now able to failover to their peer in the cluster. Providing that the Virtual System is connected to a distinct physical interface or VLAN interface, only the Virtual System fails-over, not the member.

**Per-member interface configuration**

Each cluster member can be assigned an interface with a unique IP address.

**More Cluster members**

A VSX Cluster can now support up to twelve members.

**Enhanced Diagnostic command**

The `cphaprob` diagnostic command has been extended to display additional data when the failover per Virtual System feature is enabled.

**Routing Enhancements**

**Default Gateway**

A default gateway is now optional. If used, the default gateway statement is configured as part of the static route entries.

**Best Match Routing**

Virtual Systems support best match routing decisions.
**NAT routes**

A Virtual System is capable of Network Address Translation (NAT) the same as a physical Firewall. When a Virtual System is connected to a Virtual Router and the Virtual System performs Static or Hide NAT to a host on a given network, NATed routes have to be forwarded to the Virtual Routers.

The NATed address can be:
- Manually added to the Virtual Router
- Defined on the Virtual System

Hide or Static NAT addresses configured on the Virtual System are automatically forwarded to the Virtual Router to which the Virtual System is directly connected. NATed addresses can be:
- A single IP (for Static NAT)
- A range of addresses (Hide NAT)
- Complete subnets (Hide NAT)

**Enhancements to SmartDefense**

VSX now supports:
- SmartDefense dynamic updates, INSPECT code and protocol updates
- SmartDefense Network Quota Logs

**Licensing**

The licensing scheme is now NGX. For more information on NGX licensing see the NGX Upgrade Guide at:

[http://www.checkpoint.com/support/technical/documents/docs_r60a.html](http://www.checkpoint.com/support/technical/documents/docs_r60a.html)

**NAT Enhancements**

- PPTP and GRE are now supported with Hide NAT.
- Automatic ARP for NAT
- Support for IP pool NAT on ClusterXL High availability deployments.
SecurePlatform Add-Ons & Enhancements

In This Section:

- Enhanced CLI
- NTP
- DHCP Relay
- Context Aware Command Line Interface
- Hardware Compatibility
- Ethernet Bridge Utility
- Ethtool Utility
- Internal Cluster IP Addresses
- Dynamic Routing

Enhanced CLI

Check Point Dynamic Routing utilizes industry standard commands for configuration. The basic features of the CLI include the following:

- Command line editing and completion
- Context Sensitive help
- Command history
- Disabling/Enabling CLI Tracing

Additional commands have been added for:

- NTP
- DHCP Relay
- Bridge support

NTP

VSX NGX supports the Network Time Protocol (NTP) to synchronize computer clock times in a network. The NTP client initiates a time request exchange with the network time server. As a result of this exchange, the client is able to calculate the link delay, its local offset, and adjust its local clock to match the clock at the server's computer.

DHCP Relay

By adding support for relaying DHCP requests as described in RFC 2131, the sysconfig command now allows the configuration of DHCP Clients and DHCP Servers on different networks.
Context Aware Command Line Interface

A new command line interface capable of distinguishing between Virtual Systems.

Hardware Compatibility

Hardware is now automatically verified for compatibility.

Ethernet Bridge Utility

A new bridge utility has been added to setup, maintain, and inspect the ethernet bridge configuration in the SPLAT kernel. An ethernet bridge is a device used to connect different ethernets together using the MAC hardware address. Each of the ethernets being connected corresponds to one physical interface in the bridge. These individual physical ethernets constitute a large logical ethernet which is the bridge network interface. With the bridge support utility, the ethernet bridge configuration in the kernel can be maintained and inspected.

Ethtool Utility

A new ethtool utility gives users control over network cards (line speed, duplex) and gather error statistics.

Vixie-Cron

Vixie-Cron, a version of cron authored by Paul Vixie, allows scheduling maintenance tasks on the module.

Internal Cluster IP Addresses

In a VSX cluster, the ifconfig command now hides the internal cluster addresses, i.e. the addresses of the physical interfaces on each cluster member that are reserved for internal VSX and ClusterXL communication, allocated addresses from a reserved IP range (IP:192.168.196.0/Netmask:255.255.252.0). The command ifconfig only displays the cluster IP address.

Dynamic Routing

SecurePlatform supports the following dynamic routing protocols:

- Unicast: OSPF, RIP, BGP
- Multicast: IGMP, PIM-SM, PIM-DM
New monitoring classes for Status Information

For SNMP users, additional status information can be obtained from enforcement modules by taking advantage of additional VSX monitoring classes in the Check Point MIB.

- Enhanced AMON information reported per Virtual Device
- Enhanced AMON/SNMP information reported for the VSX gateway.
- Enhanced SNMP support allows monitoring of traffic statistics per Virtual System

For more information see the guide to the Check Point MIB at: