Upgrading Check
Point VPN-1/FW-1
v4.1 to NG FP2: with
and without Nokia

N450854001
Published September 2002
Upgrading Check Point VPN-1/FW-1 v4.1 to NG FP2: with and without Nokia Horizon Manager

Upgrading a large installation of firewall platforms from Check Point's FW-1/VPN-1 product v4.1 to the latest NG FP2, without Nokia Horizon Manager (NHM), is neither an easy nor a quick task. Both Solaris and Windows-based servers acting as a FW-1 enforcement point require individual upgrades to the base NG version before they can take advantage of the Check Point SmartUpdate application.

In comparison, NHM allows a firewall administrator to simultaneously upgrade large groups of local or remote Nokia network security platforms (NSPs) to the latest version of Check Point FW-1/VPN-1 (and the IPSO operating system) quickly, easily, and securely. This capability enables the administrator to effortlessly stay current with the Check Point release cycle and ensures the rapid deployment of security fixes to the Nokia NSP.

Nokia IPSO

You can complete the following procedure on one computer at a time or on many computers simultaneously by using Nokia Horizon Manager.

To upgrade an enforcement point running on any IPSO-based network security platform

1. Upgrade to NG FP2 with the comprehensive bundle available from the Check Point support site.
2. Run cpconfig (to establish licensing and Secure Internal Communications).
   This step is required for the FW-1 management server to communicate with the enforcement module.
3. Reboot the device.
4. Establish communication with the NSP from the FW-1 management server.
Nokia Horizon Manager can perform steps 1 through 3 for as many as 2500 Nokia NSPs. This means that you can upgrade any Nokia NSP from Check Point FW-1/VPN-1 v4.1 to NG FP2 in four simple steps: three from the Horizon Manager console and a single action performed on the FW-1 management server. Moreover, Horizon Manager does not require that you install any software on the NSP platform to perform a product installation or upgrade. Once NHM knows that a Nokia NSP exists, it can perform actions on it.

All the actions between Horizon Manager and the network security platforms take advantage of the IPSO built-in security protocols to establish secured communications. This extends the network security layer outward from the firewall enforcement points to the Horizon Manager console and further protects the network.

**Upgrading Sun Solaris**

You should upgrade to service pack 6 of FW-1/VPN-1 v4.1 on a Solaris platform that acts as an enforcement point. Service pack 6 is the most recent service pack. Fortunately, you can directly upgrade a Check Point FW-1/VPN-1 v4.1 SP2 or later to this service pack. That is, you can apply FW-1 v4.1 SP6 to all service packs before SP6 to SP2. Additionally, you should upgrade the Solaris platform to Solaris 8 before the NG installation, because full Check Point installation support (that is, installation wrappers) requires Solaris 8, using a 64-bit kernel, and NG FP3 is not supported on Solaris 7.

You must perform the following procedure individually for each Solaris server that acts as an FW-1/VPN-1 enforcement point.

**To upgrade to service pack 6**

1. Upgrade to Solaris 8 and apply the necessary patches (see the Check Point release notes).
2. Install the SVN Foundation (NG FP1) application.
3. Install the rest of the desired FW-1/VPN-1 applications (NG FP1) on the server.
4. Run cpconfig (for licensing and Secure Internal Communications).
   This step is required for the FW-1 management server to communicate
   with the enforcement module.

5. Reboot the server.

Perform the following procedure from a Check Point management
server.

**To complete the upgrade**

1. Establish communication with the enforcement point from the FW-1
   management server.

2. Use SmartUpdate to update all Check Point products on all the
   enforcement points to NG FP2.

3. Reboot the server.

4. Establish communication with the network security platform from the
   FW-1 management server.

There is no direct upgrade path for Check Point FW-1/VPN-1 v4.1 to
NG FP2 on a Solaris-based system. You cannot use SmartUpdate used

to upgrade Check Point FW-1/VPN-1 v4.1 to an NG platform. While
SmartUpdate allows the firewall administrator to remotely and simulta-
neously upgrade any Check Point product on a Solaris platform, it
requires that the SVN Foundation (cpshared_NG...Solaris.tgz) be
installed, configured, and active on the target servers. This requires that
the firewall administrator install Check Point FW-1/VPN-1 NG FP1 on
each Solaris-based enforcement point individually.

**Microsoft Windows**

The general upgrade procedure for a Windows server acting as an FW-1/
VPN-1 enforcement point is essentially the same as for a Solaris server.

Perform the following procedure individually for each Windows server that
acts as an enforcement point.
**Upgrading a Windows server**

1. Install the SVN Foundation (NG FP1) application.
2. Install the rest of the FW-1/VPN-1 applications (NG FP1) on the server.
3. Run cpconfig (for licensing and Secure Internal Communications).
   - This step is required for the FW-1 management server to communicate with the enforcement module.
4. Reboot the server.

**To complete the upgrade**

1. From a Check Point management server, establish communication with the enforcement point from the FW-1 management server
2. Use SmartUpdate to update all Check Point products on all the enforcement points to NG FP2.
3. Reboot the server.
4. Establish communication with the network security platform from the FW-1 management server

There is no direct upgrade path for Check Point FW-1/VPN-1 v4.1 to NG FP2 on a Windows-based system. You cannot use SmartUpdate used to upgrade Check Point FW-1/VPN-1 v4.1 to an NG platform. While SmartUpdate allows the firewall administrator to remotely and simultaneously upgrade any Check Point product on a Windows platform, it requires that the SVN Foundation (cpshared_NG...win_package.tgz) be installed, configured, and active on the target servers. This requires that the firewall administrator visit each Windows-based enforcement point individually and install Check Point FW-1/VPN-1 NG FP1.

**Summary**

A network administrator's time is the most restricted and valuable resource in any installed network. Downtime for maintenance is to be avoided as much as possible. Conversely, maintaining concurrency with the latest security patches
and fixes is of the utmost importance for network stability and security. The combination of the Nokia network security platforms and Nokia Horizon Manager minimizes maintenance downtime while ensuring enhanced network visibility and uptime.
Upgrading Check Point VPN-1/FW-1 4.1 to NG FP2: with and without Nokia Horizon Manager