

CHAPTER 4: CONFIGURING AND MANAGING INTERSPECT

.....

An InterSpect appliance is designed to be placed into a network out of the box. While there is minimal configuration required for the appliance to be fully functional, the InterSpect appliance can also be integrated into an existing security infrastructure protected by VPN-1 NGX. The InterSpect appliance ships in Switch mode by default. If another mode is desired, the appliance will require configuration before placement in the network. For InterSpect NGX, InterSpect can be managed centrally using SmartCenter Server, or locally via a client connection from the InterSpect SmartConsole.

Objectives

1. Set up and configure InterSpect using the Command Line Interface and/or Web GUI, according to environmental requirements.
2. Select local management (SmartDashboard directly to InterSpect) versus central management (SmartDashboard control via SmartCenter).
3. Configure InterSpect for either locally or centrally managed logging, according to business requirements.



Key Terms

- Console connection
- Secure Shell (SSH)
- sysconfig
- InterSpect SmartDashboard
- Central management
- Local management
- Secure Internal Communications (SIC)



CONFIGURATION AND SETUP

Configuration and setup of InterSpect involves several phases: the initial hardware installation, operating-system level configuration, further configuration via Check Point setup scripts, and configuration of zones, profiles, and SmartDefense via the InterSpect SmartDashboard (when applicable).

Initial Configuration

The initial configuration of an InterSpect appliance involves using either a console connection; installing a keyboard, video, and mouse; or using a Secure Shell (SSH) to connect to a default management interface (192.168.1.1/24). A **console connection** is a method of connecting and managing a system using a serial connection port and a terminal program. **SSH** is a UNIX shell for logging into and executing commands on a remote computer. SSH is intended to replace rlogin and rsh, and provide secure, encrypted communications between two untrusted hosts over an unsecured network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel.

Once the system has completed booting, you are prompted for basic setup information. If the default information is acceptable, simply select **OK** and the system completes its configuration. To connect to the console, use the settings **9600 8N1**, which means 9600 BPS, 8 bits, no parity, 1 stop bit.

Once configuration is complete and the appliance has rebooted, you may continue configuring the system. The default username is “admin”, and the password is “admin”. You are required to change the default password the first time you log in to the InterSpect appliance. The new password is compared against a dictionary to verify it is not a well-known or commonly used word. It is also possible to change the default username from admin if desired.

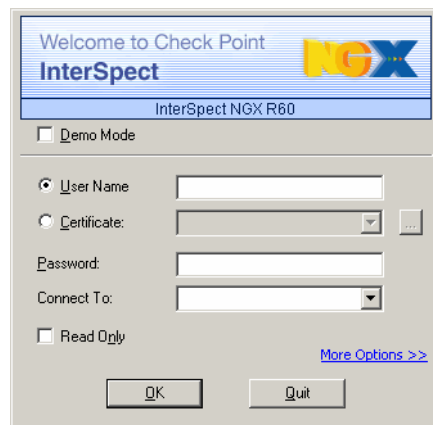
Basic Configuration

Basic configuration of an InterSpect appliance is accomplished using **sysconfig**, the utility for configuring all functions of the Check Point InterSpect operating system, SecurePlatform. This includes setting up various IP addresses for the bridge (br0), DNS, and other networking aspects. Configuration of Check Point products is also possible, but the InterSpect appliance is already configured to run InterSpect.

Once console configuration is complete, the Administrator can connect to the appliance via HTTPS to the management-port IP address. This connection allows the Administrator to download the **InterSpect SmartDashboard** management client for further configuration changes and customization. The InterSpect SmartDashboard is used to configure zones and profiles, determine the ports used for specific zones, and to configure SmartDefense and Web intelligence protections.

Logging into SmartDashboard

The InterSpect SmartDashboard login window is very similar to the login window of other Check Point products:



InterSpect SmartDashboard Login Window

The following information is required:

- User name (**isadmin**)
- Password or Certificate
- IP address of the management port

Once authentication takes place, the Administrator is presented with the initial status window of the InterSpect appliance.



MANAGING INTERSPECT WITH SMARTCENTER SERVER



Overview

Although this course focuses primarily on InterSpect as a separately managed device within a network infrastructure, InterSpect is fully capable of being incorporated into an existing Check Point management framework. The difference between these two management philosophies for the product are defined as local management and central management.

InterSpect NGX R60 can be **centrally managed** from SmartCenter Pro and SmartCenter Enterprise NGX R60a or higher.

Under **local management**, the SmartConsole management client connects directly to the InterSpect appliance. Management activities, such as performing SmartDefense dynamic updates, viewing logs, and activating settings are performed from the local SmartDashboard.

Understanding Central Management

Under central management, multiple InterSpect appliances are managed from the SmartDashboard, i.e., connected to the central-management SmartCenter Server (the central SmartDashboard). From the central SmartDashboard of SmartCenter Pro and SmartCenter Enterprise NGX R60a or higher, a network object for each InterSpect appliance must be defined. A separate SmartDashboard session can then be launched for each InterSpect object created.

From the Central SmartDashboard you can:

- Perform a SmartDefense update and simultaneously activate settings for all or some InterSpect appliances. If updates are configured for a large number of appliances, they are performed in batches. The update process itself can be aborted if necessary. This aborts pending updates, but those that are actually in progress continue.

- Monitor the performance and security state of InterSpect traffic, by means of SmartView Monitor.
- Manage an InterSpect appliance 2.0 or higher, exactly as if locally connected.

Secure Internal Communications (SIC)

When Check Point products are configured to work in the central-management model, they communicate using Check Point's **Secure Internal Communications (SIC)**, a Certificate based encrypted system allowing for secure, authenticated communications, even in cases where Check Point products are located in different physical locations.

SIC between the central-management server and each InterSpect appliance is required to allow:

- Sending logs to the central-management server (SmartCenter Server) and/or a remote log server.
- Viewing system status using SmartView Monitor.
- Cooperative enforcement with Integrity Server, when InterSpect is centrally managed.



SIC is not required to perform a SmartDefense update, to activate settings from the central management server, or to use the InterSpect SmartDashboard.

Defining the InterSpect Central-Management Network Object

From the SmartDashboard menu of the central-management server:

1. Define the InterSpect object: Right-click the **Network Objects** tree, and select **New > Check Point > InterSpect Device**. The **InterSpect Properties** window opens.
2. Name the object. Object names must start with a letter.
3. Specify the IP address and version of the InterSpect management interface. A SmartDefense Dynamic Update can be performed for all versions. You can manage all InterSpect appliances version 2.0 or higher.



4. Specify the InterSpect SmartConsole Administrator username and password. Use the Administrator that was defined using the InterSpect SmartDashboard, as described in the InterSpect *Getting Started Guide*.
5. Install the objects database by choosing **Policy > Install Database**.

Performing a Central SmartDefense Update

From the SmartDashboard menu of the central-management server:

1. Right-click one of the InterSpect network objects, and select **InterSpect Dynamic Updates**.
2. In the **InterSpect Dynamic Updates** window, select the InterSpect appliance or appliances on which to perform a SmartDefense update, and those on which you wish to activate settings. Click **OK**.
3. In the **User Center Login** window, enter your credentials and click **OK**. The update begins. Track the progress in the **Progress** window.

Centrally Managing an InterSpect Appliance

From the SmartDashboard client of the central-management server:

1. Right-click an InterSpect network object, and select **Manage InterSpect**.
2. The InterSpect SmartDashboard opens. Manage the appliance as you would locally.

INTERSPECT LOGGING

.....

Logging is a vital component of InterSpect and SmartDefense. Log records can be used to determine the types of attacks occurring against the protected InterSpect zones. Log records can also be used after the fact for forensic examinations of an attack to determine the instigator, or, in cases of a worm infection, the “zero patient” host that introduced the worm to the network. Logs can also be processed by Check Point Eventia Reporter into reports to show traffic and attack patterns.

Log-Handling Options

There are two options for handling logs:

- Storing logs locally on the InterSpect appliance
- Sending logs to the central-management server (SmartCenter Server) and/or a remote log server

Either or both options can be configured. To send logs to the central-management server, SIC must be established between the central-management server and each InterSpect appliance. Logs can also be viewed using SmartView Tracker. Searches can be customized to address specific tracking needs. Logs can be exported to text files or to an external Oracle database. Logs are organized in files according to the order in which they arrive at the log server. All new logs are saved to the **fw.log** file, except for audit (SmartCenter-related) logs, which are saved to the **fw.adt.log** file.