Security Management Overview.................................................................8
  Introduction ...............................................................................................8
  Deployments ...............................................................................................8
  Some Basic Concepts and Terminology .........................................................9
Management Software Blades .........................................................................10
Login Process ................................................................................................12
  Overview ......................................................................................................12
  Authenticating the Administrator .................................................................12
  Authenticating the Security Management Server Using its Fingerprint .......12
Tour of SmartDashboard ..................................................................................13
  SmartDashboard and Objects .......................................................................13
  Managing Objects ........................................................................................15
  Configuring Objects .....................................................................................15
  Changing the View in the Objects Tree .........................................................15
  Groups in the Network Objects Tree .............................................................17
Securing Channels of Communication (SIC) ..................................................20
  The SIC Solution ........................................................................................21
  The Internal Certificate Authority (ICA) .......................................................21
  Initializing the Trust Establishment Process ...............................................21
  Understanding SIC Trust States .................................................................22
  Testing the SIC Status ................................................................................22
  Resetting the Trust State ............................................................................22
  Troubleshooting SIC ..................................................................................22
Network Topology ..........................................................................................23
Managing Users in SmartDashboard .............................................................24
  User Management Requirements ...............................................................24
  The Check Point User Management Solution ..............................................24
  Users Database ............................................................................................24
  User and Administrator Types .....................................................................25
  Configuring User Objects ..........................................................................25
Working with Policies .....................................................................................27
  Overview ......................................................................................................27
  To Install a Policy Package ..........................................................................28
  To Uninstall a Policy Package .....................................................................28
  Installing the User Database .......................................................................28
Policy Management ..........................................................................................30
  The Need for an Effective Policy Management Tool ....................................30
  The Check Point Solution for Managing Policies .........................................30
    Policy Management Overview ..................................................................30
    Policy Packages .......................................................................................31
    Dividing the Rule Base into Sections using Section Titles .........................33
    Querying and Sorting Rules and Objects ..................................................33
Policy Management Considerations ..............................................................34
  Conventions ...............................................................................................34
Policy Management Configuration ...............................................................34
  Policy Package ...........................................................................................34
  Rule Sections .............................................................................................35
  Querying the Rule Base ..............................................................................35
  Querying and Sorting Objects ....................................................................36
SmartMap .......................................................................................................38
  Overview of SmartMap ..............................................................................38
  The SmartMap Solution ..............................................................................38
Chapter 1

Security Management Overview

In This Chapter

<table>
<thead>
<tr>
<th>In This Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>8</td>
</tr>
<tr>
<td>Management Software Blades</td>
<td>10</td>
</tr>
<tr>
<td>Login Process</td>
<td>12</td>
</tr>
<tr>
<td>Tour of SmartDashboard</td>
<td>13</td>
</tr>
<tr>
<td>Securing Channels of Communication (SIC)</td>
<td>20</td>
</tr>
<tr>
<td>Network Topology</td>
<td>23</td>
</tr>
<tr>
<td>Managing Users in SmartDashboard</td>
<td>24</td>
</tr>
<tr>
<td>Working with Policies</td>
<td>27</td>
</tr>
</tbody>
</table>

Introduction

To make the most of Check Point products and all their capabilities and features, you must be familiar with some basic concepts and components. This chapter includes an overview of usage, and describes the terminology and procedures that will help you administer your Check Point Security Gateways.

Deployments

There are two basic deployments:

- **Standalone deployment** - where the gateway and the Security Management server are installed on the same machine.
- **Distributed deployment** - where the gateway and the Security Management server are installed on different machines (see the figure).

A typical deployment
In the figure, there are two gateways. Each gateway connects to the Internet on one side, and to a LAN on the other.

It is possible to create a Virtual Private Network (VPN) between the two gateways, to secure all communication between them.

The Security Management server is installed in the LAN, so that it is protected by a Security Gateway. The Security Management server manages the gateways and allows remote users to connect securely to the corporate network. SmartDashboard may be installed on the Security Management server or on any other machine.

In addition to Check Point gateways, other OPSEC-partner modules (for example, an AntiVirus Server) can be deployed in order to complete the network security in collaboration with the Security Management server and its gateways.

Some Basic Concepts and Terminology

- **Administrators** are the designated managers of SmartConsole. They are assigned different levels of access permissions, which define their ability to view and/or modify data using the SmartConsole. At least one administrator must have full Read/Write permissions so that he or she can manage the Security Policy.

- **Configuration** is the process by which Check Point Security Gateways and Security Management servers are configured using the Check Point Configuration Tool. This tool runs immediately after the initial stages of installation are complete. However, it can be run and modified at any time. During the configuration process, the major attributes of the installed product are defined, such as the definition of Administrators, Fingerprint (for first time Security Management server identity verification), as well as features such as Management High Availability.

- **Installation** is the process by which the Check Point product components are installed on a computer. Check Point products are based on a 3-tier technology architecture where a typical Check Point deployment is composed of a gateway, the Security Management server and a SmartConsole (usually SmartDashboard). There are several different ways to deploy these components:
  - A **standalone deployment** is the simplest deployment, where the components that are responsible for the management of the Security Policy (the Security Management server, and the gateway) are installed on the same machine.
  - A **distributed deployment** is a more complex deployment where the gateway and the Security Management server are deployed on different machines.
    In all deployments, SmartConsole can be installed on any machine, unless stated otherwise.

- **Licenses** are required in order to use certain Check Point software blades and features. It is recommended to use SmartUpdate for license management.
Management Software Blades

Software Blades are independent and flexible security modules that enable you to select the functions you want to build a custom Check Point Security Gateways. Software Blades can be purchased independently or as pre-defined bundles.

The following Security Management Software Blades are available:
<table>
<thead>
<tr>
<th>Security Management Software Blades</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Policy Management</td>
<td>Gives you control over configuring and managing even the most complex security deployments. Based on the Check Point unified security architecture, the Network Policy Management Software Blade provides comprehensive security policy management using SmartDashboard - a single, unified console for all security features and functionality.</td>
</tr>
<tr>
<td>Endpoint Policy Management</td>
<td>Enables you to centrally manage the security products you use on your organization's end-user devices. This means that you can take and keep control of computing devices and the sensitive information they contain.</td>
</tr>
<tr>
<td>Logging &amp; Status</td>
<td>Provides comprehensive information on security activity in the form of logs and a complete visual picture of changes to gateways, tunnels, remote users, and security activities.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Shows a complete picture of network and security performance, enabling fast response to changes in traffic patterns or security events.</td>
</tr>
<tr>
<td>Management Portal</td>
<td>With the Management Portal Software Blade, the security team can extend browser-based management access to outside groups such as technical support staff or auditors yet maintain centralized control of policy enforcement. Management Portal users can view security policies, status of all Check Point products and administrator activity as well as edit, create and/or modify internal users, and manage firewall logs.</td>
</tr>
<tr>
<td>User Directory</td>
<td>Enables Check Point Security Gateways to leverage LDAP-based user information stores, eliminating the risks associated with manually maintaining and synchronizing redundant data stores. With the Check Point User Directory Software Blade, Check Point Security Gateways become full LDAP clients which communicate with LDAP servers to obtain identification and security information about network users.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Provides centralized administration and provisioning of Check Point security devices via a single management console. Using profiles, a network administrator can easily deploy security policy or configuration settings to multiple, geographically distributed devices. The Check Point Provisioning Software Blade also provides centralized backup management and a repository of device configurations so administrators can easily apply existing configurations to new devices.</td>
</tr>
<tr>
<td>SmartReporter</td>
<td>Centralizes reporting on network, security, and user activity and consolidates the data into concise predefined and custom-built reports. Easy report generation and automatic distribution save time and money.</td>
</tr>
<tr>
<td>SmartEvent</td>
<td>The Event Correlation Software Blade provides centralized, real-time security event correlation and management for Check Point security gateways and third-party devices. Automated aggregation and correlation of data not only substantially minimizes the time spent analyzing data but also isolates and prioritizes the real security threats.</td>
</tr>
<tr>
<td>SmartEvent Intro</td>
<td>Complete IPS or DLP event management system providing situational visibility, easy to use forensic tools, and reporting.</td>
</tr>
</tbody>
</table>

To verify which and how many Software Blades are currently installed on the Security Management Server, look at the SmartDashboard representation of the Security management server. In the General Properties
page of the Security management server, the Management tab of the Software Blades section shows all enabled management Software Blades.

In a High Availability environment the Software Blade must be enabled on each High Availability Management.


Login Process

Overview

The login process, in which administrators connect to the Security Management server, is common to all Check Point SmartConsole applications (SmartDashboard, SmartUpdate, etc.). This process consists of a bidirectional operation, in which the administrator and the Security Management server authenticate each other and create a secure channel of communication between them using Secure Internal Communication (SIC). Once both the administrator and the Security Management server have been successfully authenticated, the Security Management server launches the selected SmartConsole.

Authenticating the Administrator

Administrators can authenticate themselves in two different ways, depending on the tool used to create them: the Check Point Configuration Tool or the SmartDashboard.

Administrators defined through the Check Point Configuration Tool authenticate themselves with a User Name and Password combination. This process is known as asymmetric SIC, since only the Security Management server is authenticated using a certificate.

Administrators defined through the SmartDashboard can authenticate themselves with a user name and password combination, or by using a Certificate. If using a certificate, the administrator browses to the certificate and unlocks it by entering its password. This process is known as symmetric SIC, since both the Security Management server and the administrator authenticate each other using certificates.

After providing the authentication information, the administrator specifies the name or IP address of the target Security Management server and clicks OK to perform the authentication. If the administrator is authenticated successfully by the Security Management server, one of the following operations takes place:

- If this is the first time this SmartConsole has been used to connect to the Security Management server, the administrator must manually authenticate the Security Management server using its Fingerprint.
- If this SmartConsole has already been used to connect to the Security Management server, and an administrator has already authenticated the Security Management server, Fingerprint authentication is performed automatically.

Authenticating the Security Management Server Using its Fingerprint

The administrator authenticates the Security Management server using the Security Management server's Fingerprint. This Fingerprint, shown in the Fingerprint tab of the Check Point Configuration Tool, is obtained by the administrator before attempting to connect to the Security Management server.

The first time the administrator connects to the Security Management server, the Security Management server displays a Fingerprint verification window. The administrator, who has the original Fingerprint on hand, compares it to the displayed Fingerprint. If the two are identical, the administrator approves the Fingerprint as valid. This action saves the Fingerprint (along with the Security Management server's IP address) to the SmartConsole machine's registry, where it remains available to automatically authenticate the Security Management server in the future.

If the Fingerprints are not identical, the administrator quits the Fingerprint verification window and returns to the initial login window. In this case, the administrator should verify the resolvable name or IP address of the Security Management server.
Tour of SmartDashboard

Objects are created by the system administrator in order to represent actual hosts and devices, as well as intangible components such as services (for example, HTTP and TELNET) and resources, (for example, URI and FTP). Each component of an organization has a corresponding object which represents it. Once these objects are created, they can be used in the rules of the Security Policy. Objects are the building blocks of Security Policy rules and are stored in the Objects database on the Security Management server.

Objects in SmartDashboard are divided into several categories which can be viewed in the different tabs of the Objects Tree.

For instance, the **Network Objects** tab represents the physical machines as well as logical components, such as dynamic objects and address ranges that make up your organization.

When creating objects the system administrator must consider the needs of the organization:

- What are the physical and logical components that make up the organization? Each component that accesses the firewall most likely needs to be defined.
- Who are the users and administrators and how should they be divided into different groups?

In other words, a substantial amount of planning should go into deciding what objects should be created and how they should be implemented.

SmartDashboard and Objects

**Introduction to SmartDashboard and Objects**

SmartDashboard is comprised of four principal areas known as panes. Each pane is labeled in the following figure:
Managing and Implementing Objects

From these panes, objects are created, manipulated, and accessed. The following section describes the functions and characteristics of each pane.

**Objects Tree Pane**

The Objects Tree is the main view for managing and displaying objects. Objects are distributed among logical categories (called tabs), such as **Network Objects** and **Services**. Each tab, in turn, orders its objects logically. For example, the **Services** tab locates all services using ICMP in the folder called **ICMP**. The **Network Objects** tab has an additional way of organizing objects; see Changing the View in the Objects Tree (on page 15) for details.

**Objects List Pane**

The Objects Tree works in conjunction with the Objects List. The Objects List displays current information for a selected object category. For example, when a Logical Server Network Object is selected in the Objects Tree, the Objects List displays a list of Logical Servers, with certain details displayed.

**Rule Base Pane**

Objects are implemented across various **Rule Bases** where they are used in the rules of the various policies. For example, Network Objects are generally used in the **Source**, **Destination** or **Install On** columns, while Time objects can be applied in any Rule Base with a **Time** column.

**SmartMap Pane**

A graphical display of objects in the system is displayed in **SmartMap** view. This view is a visual representation of the network topology. Existing objects representing physical components such as gateways or Hosts are displayed in SmartMap, but logical objects such as dynamic objects cannot be displayed.
Managing Objects

The Objects Tree is the main view for adding, editing and deleting objects, although these operations can also be performed from the menus, toolbars and the various views such as in Rule Bases or in SmartMap.

Create an Object via the Objects Tree

To add a new object, right-click the object type that you would like to add. For example, in the Network Objects tab, right-click Networks and select New Network from the displayed menu.

Edit an Object via the Objects Tree

To edit an existing object, right-click the desired object in the Objects Tree and select Edit from the displayed menu, or double-click on the object that you would like to modify.

Delete an Object via the Objects Tree

To delete an existing object, right-click on the object in the Objects Tree and click Delete from the displayed menu.

Configuring Objects

An object consists of one or more tabs and/or pages. It is in these tabs and/or pages that the object settings are configured.

A Typical Object Configuration

To define and configure a new Security gateway object:

1. To create a new Security Gateway in the Objects Tree, right-click on Check Point, then select Security Gateway.
   A window is displayed which allows you to configure this object using a helper wizard, or manually, via the Classic method.
2. Select the Classic method. The Security Gateway is displayed with the following four default pages:
   • General Properties — The required values of most new objects are a name and an IP address. In this window you should also select the Check Point software blades that are installed on the Security Gateway. For this object to communicate with the Security Management server, you must initialize Secure Internal Communication (SIC) by clicking Communication.
   • Topology — Enter the interfaces that make up the network topology of your organization.
   • NAT — If relevant, configure this object for NAT and anti-spoofing purposes.
   • Advanced — If relevant, configure this object for use of the SNMP daemon. It is also possible to define the object as a Web, Mail, or DNS Server.
3. Once you have configured the object, click OK to apply the changes to the new object. This object will be added to the Network Objects tab of the Objects Tree and to the Objects List.

Note - It is possible to clone a Host object and a Network object (that is, duplicate the object). To do this, right-click the Host or Network object you would like to duplicate, select Clone... and enter a new name.

Changing the View in the Objects Tree

The Network Objects Tree provides two possible ways of viewing and organizing network objects. The first is known as Classic View, which automatically places each object in a predefined logical category. The second is Group View, which provides additional flexibility in organizing objects by groups.
Classic View of the Objects Tree

In Classic View, network objects are displayed beneath their object type. For example, a corporate mail server would appear under the **Node** category.

**Nodes in the Objects Tree**

Check Point management stations and gateways appear under the category **Check Point**, DAIP servers appear in the category **Dynamic Objects**, etc. Organizing objects by category is preferred for small to medium sized deployments. SmartDashboard opens to Classic View by default unless set to Group View.

Group View of the Objects Tree

In Group View, network objects are organized by the Group Objects to which they belong. For instance, a group called **GW-group** could include all of the gateway objects in an organization.

**Group View**

Group View provides the flexibility to display objects in a manner pursuant to the specific needs of your organization. That manner could be by function, as the gateway group above describes, by regional distributions of resources, or any number of other groupings. Group View is especially useful for larger deployments that could benefit from grouping objects in this way.

Any objects not associated with a group appear as they would in Classic View, in the appropriate logical category under the category **Others**.

You can switch to Group View by right-clicking on **Network Objects**, and selecting **Arrange by groups**. As changing views can at first be disorienting, a warning message appears.
Warning Dialog Box Before Entering Groups View

Click **OK** and note that the **Network Objects** tab is now arranged by group. If no groups have been created, the order is similar to that of Classic View, with the addition of the category **Others**.

Switch to Arrange by Group

When you begin adding groups, they appear above the **Others** category.

**Removing Objects from Groups while in Group View**

To remove an object from a group, from the Objects Tree, right-click on the object and select **Remove From Group** in the context menu. This deletes the group membership of the object, but not the object itself.

**Groups in the Network Objects Tree**

**Defining and Configuring a Group Object**

To create a new group in the Objects Tree, right-click on **Network Objects**, then select **New > Groups > Simple Group**....

The **Group Properties** window opens and allows you to configure the group. Give the group a name, select the objects you want in the group from the **Not in Group** pane, and click **Move >**. To save your new group, click **OK**.

Note that when you select a group in the Objects Tree, the group's network objects appear in the Objects List, as depicted in the following figure.
A Group's Network Objects Appear in the Objects List

You can create groups that are members of other groups. In the next figure, the nested group Alaska is shown as a member of GW-group in the Objects List.

Group within a Group

Group Sort Order

The Network Objects tree can be sorted by type, name, and color.

- **Sort Tree by Type** is the default view where objects are arranged in logical categories.
- **Sort Tree by Name** removes all categories from the Network Objects pane and orders objects alphabetically. Group objects are always listed first, however.
- **Sort Tree by Color** removes all categories from the Network Objects pane and orders objects by color. As in Sort by Name, group objects are listed first.

To change the sorting order of the Network Objects tree, right-click on any category or object in the Network Objects tree and select one of the three Sort Tree by options.

Assigning and Removing Group Membership

You can assign group membership to an object by dragging it to a group, as well as by copying and pasting. Removing it from the group, however, is performed by editing the group object.

Showing the Group's Hierarchy

You can set groups to display their member objects within the Objects Tree. Thus, in a glance you can see each group and the network objects associated with it. Each object added appears in its logical category under the group. For example, in the following figure, GW-group contains the folder Check Point and its member gateway objects.
Group Hierarchy

This ability to view group member objects in a hierarchical fashion is useful in providing context to each device. Grouping objects in meaningful ways can make locating and working with them faster and easier. A remote gateway object in a group called **GW-group** is easily located, for instance.

Also, when creating nested groups (groups within groups), displaying their hierarchy naturally adds clarity to the organizational structure. In the figure, group **GW-group** is a member of group **Texas**.

Group within a Group in Hierarchical View

Showing the group hierarchy adds additional functionality as well. For instance, right-clicking on a group object provides the option to create a new network object that will automatically be assigned membership in the group.

It also allows groups to be sorted individually. By right-clicking on a group object, you can choose to sort objects in a manner independent of how the tree or other groups are sorted. You can sort each group by type, name or color, or as the Objects Tree is sorted.

To enable group hierarchy, right-click on either the **Groups** category or a group object and select **Show groups hierarchy**.

Removing an Object from a Group

When showing group hierarchy, an object can be removed from a group by right-clicking on the object in the Objects Tree and selecting **Remove from group**.

Group Conventions

You can configure a group object to have SmartDashboard prompt you whenever you create a network object whose criteria match certain properties you define as characteristic of the group. If you select **Suggest to add objects to this group**, the **Group Properties** window then shifts to display matchable properties (see the following figure).
Group Properties

Use the drop-down menus to choose any combination of name, color, and network to set the appropriate condition to be a member of this group. For example, say you set as a matchable property the network object Corporate-dmz-net. Subsequently, each time you create an object with an IP address on this network, SmartDashboard will suggest to include the new object in this group. Answering yes places the object in the group.

If an object matches the properties of several groups, the Groups Selection Dialog window appears (see the following figure).

Figure 1-1 Groups Selection Dialog Window

If the list of matching groups includes a group to which you do not want to assign the object, set that group’s Action property to Don’t Add, and click OK.

If you alter the properties of an object in such a way that it no longer matches the parameters of the group, SmartDashboard alerts you to the fact and asks if you want to remove the object from the group. Removing an object from a group in no way deletes the object or otherwise changes it. If an object does not belong to any other group, you can locate it in its logical category under Others.

Securing Channels of Communication (SIC)

The Security Management server must be able to communicate with all the gateways and partner-OPSEC applications that it manages, even though they may be installed on different machines. The interaction must take place to ensure that the gateways receive all the necessary information from the Security Management
server (such as the Security Policy). While information must be allowed to pass freely, it also has to pass securely.

This means that:

- The communication must be encrypted so that an impostor cannot send, receive or intercept communication meant for someone else.
- The communication must be authenticated, so that there can be no doubt as to the identity of the communicating peers.
- The transmitted communication should have data integrity, that is, the communication has not been altered or distorted in any form.
- The SIC setup process allowing the intercommunication to take place must be user-friendly.

If these criteria are met, secure channels of communication between inter-communicating components of the system can be set up and enforced to protect the free and secure flow of information.

The SIC Solution

Secure communication channels between Check Point nodes (such as Security Management server, gateways or OPSEC modules) can be set up using Secure Internal Communication (SIC). This ensures that these nodes can communicate freely and securely using a simple communication initialization process.

The following security measures are taken to ensure the safety of SIC:

- Certificates for authentication
- Standards-based SSL for the creation of the secure channel
- 3DES for encryption.

The Internal Certificate Authority (ICA)

The ICA is created during the Security Management server installation process. The ICA is responsible for issuing certificates for authentication. For example, ICA issues certificates such as SIC certificates for authentication purposes to administrators and VPN certificates to users and gateways.

Initializing the Trust Establishment Process

The purpose of the Communication Initialization process is to establish a trust between Security Management server and the Check Point gateways. This trust enables these components to communicate freely and securely. Trust can only be established when the gateways and the Security Management server have been issued SIC certificates. The SIC initialization process occurs as follows:

Note - In order for SIC between the Management and the Gateway to succeed, their clocks must be properly and accurately synchronized.

1. In the Check Point Configuration Tool, when the Security Management server is installed, the Internal Certificate Authority (ICA) is created. After the ICA is created, it issues and delivers a certificate to the Security Management server.
2. SIC can be initialized for every gateway in the Secure Internal Communication tab of the Check Point Configuration tool. An Activation Key must be decided upon and remembered. This same Activation Key must be applied on the appropriate network object in SmartDashboard. At this point only the Gateway side has been prepared. The Trust state remains Uninitialized.
3. In SmartDashboard, connect to the Security Management server. Create a new object that represents the gateway. In the General Properties page of the gateway, click Communication to initialize the SIC procedure.
4. In the Communication window of the object, enter the Activation Key that you created in step 2.
5. To continue the SIC procedure, click Initialize. At this point the gateway is issued a certificate by the ICA. The certificate is signed by the ICA.
6. SSL negotiation takes place after which the two communicating peers are authenticating with their Activation Key.
7. The certificate is downloaded securely and stored on the gateway.
8. After successful Initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate, signed by the same ICA. The Activation Key is deleted. The SIC process no longer requires the Activation Key, only the SIC certificates.

Understanding SIC Trust States

When the SIC certificate has been securely delivered to the gateway, the Trust state is Trust Established. Until that point the gateway can be in one of two states: Uninitialized or Initialized but not trusted. Initialized but not trusted means that the certificate has been issued for the gateway, but has not yet been delivered.

Testing the SIC Status

The SIC status reflects the state of the Gateway after it has received the certificate issued by the ICA. This status conveys whether or not the Security Management server is able to communicate securely with the gateway. The most typical status is Communicating. Any other status indicates that the SIC communication is problematic. For example, if the SIC status is Unknown then there is no connection between the Gateway and the Security Management server. If the SIC status is Not Communicating, the Security Management server is able to contact the gateway, but SIC communication cannot be established. In this case an error message will appear, which may contain specific instructions how to remedy the situation.

Resetting the Trust State

Resetting the Trust State revokes the gateway's SIC certificate. This must be done if the security of the gateway has been breached, or if for any other reason the gateway functionality must be stopped. When the gateway is reset, the Certificate Revocation List (CRL) is updated to include the name of the revoked certificate. The CRL is signed by the ICA and issued to all the gateways in this system the next time a SIC connection is made. If there is a discrepancy between the CRL of two communicating components, the newest CRL is always used. The gateways refer to the latest CRL and deny a connection from an impostor posing as a gateway and using a SIC certificate that has already been revoked.

**Important** - The Reset operation must be performed on the gateway’s object, using SmartDashboard, as well as physically on the gateway using the Check Point Configuration Tool.

To reset the Trust State in SmartDashboard:
1. In SmartDashboard, in the General Properties window of the gateway, click Communication.
2. In the Communication window, click Reset.
3. To reset the Trust State in the Check Point Configuration tool of the gateway, click Reset in the Secure Internal Communication tab.
4. Install the Security Policy on all gateways. This deploys the updated CRL to all gateways.

Troubleshooting SIC

If SIC fails to Initialize:
1. Ensure connectivity between the gateway and Security Management server.
2. Verify that server and gateway use the same SIC activation key.
3. If the Security Management server is behind another gateway, make sure there are rules that allow connections between the Security Management server and the remote gateway, including anti-spoofing settings.
4. Ensure the Security Management server’s IP address and name are in the /etc/hosts file on the gateway.
   - If the IP address of the Security Management server undergoes static NAT by its local Security Gateway, add the public IP address of the Security Management server to the /etc/hosts file on the remote Security Gateway, to resolve to its hostname.
5. Check the date and time of the operating systems and make sure the time is accurate. If the Security Management server and remote gateway reside in two different time zones, the remote gateway may need to wait for the certificate to become valid.
6. On the command line of the gateway, type: `fw unloadlocal` This removes the security policy so that all traffic is allowed through.

7. Try again to establish SIC.

If RemoteAccess users cannot reach resources and SSL VPN is enabled:
- After you install the certificate on a Security Gateway, if the SSL VPN Software Blade is enabled, you must install Policy on the gateways again.

---

**Network Topology**

The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:

- Correctly enforce the Security Policy.
- Ensure the validity of IP addresses for inbound and outbound traffic.
- Configure a special domain for Virtual Private Networks.

Each component in the network topology is distinguished on the network by its IP address and netmask. The combination of objects and their respective IP information make up the topology. For example:

- The IP address of the LAN is 10.111.254.0 with Net Mask 255.255.255.0.
- A Security Gateway on this network has an external interface with the following IP address 192.168.1.1, and an internal interface with 10.111.254.254.

In this case, there is one simple internal network.

In more complicated scenarios, the LAN is composed of many different networks (see the following figure).

**Figure 1-2** A complex topology

The internal network is composed of the following:

- The IP address of the first is 10.11.254.0 with Net Mask 255.255.255.0.
- The IP address of the second is 10.112.117.0 with Net Mask 255.255.255.0.
- A Security Gateway that protects this network has an external interface with IP address 192.168.1.1, and an internal interface with 10.111.254.254.

In this case the system administrator must define the topology of the gateway accordingly.

In SmartDashboard:

- An object should be created to represent each network. The definition must include the network's IP address and netmask.
- A group object should be created which includes both networks. This object represents the LAN.
- In the gateway object, the internal interface should be edited to include the group object. (In the selected gateway, double-click on the internal interface in the **Topology** page. Select the group defined as the specific IP addresses that lie behind this interface).
Managing Users in SmartDashboard

User Management Requirements
Your network can be accessed and managed by multiple users and administrators. To manage your network securely and efficiently, you must:

- Centrally manage all users through a single administrative framework.
- Ensure only authenticated users can access your network and allow users to securely access your network from remote locations.

The Check Point User Management Solution
Check Point users can be managed using either the Lightweight Directory Access Protocol (LDAP) or SmartDashboard.

SmartDirectory (LDAP)
LDAP is a standardized protocol that makes a single Users Database available to multiple applications (for example, email, domains, firewalls, etc.) and requires a special deployment (in addition to the Security Management deployment). For information on managing users through LDAP, see SmartDirectory (LDAP) and User Management (on page 115).

SmartDashboard
The Check Point user management solution is part of SmartDashboard. Users, Administrators and their groups are managed as objects, using the standard object administration tools: the Objects Tree pane and the Objects Manager window.

- The Objects Tree pane (Users and Administrators tab):
  - Provides a graphical overview of all users and administrators.
  - Allows you to manage users and administrators by right-clicking the relevant folder (for example, Administrator, Administrator Groups, External User Profiles, etc.) and selecting the appropriate command (Add, Edit, Delete, etc.) from the menu.

- The Objects Manager (Users and Administrators window):
  - Lists all users and administrators (you can filter this list to focus on specific types of users or administrators).
  - Allows you to define new objects using the New... menu, and to delete or modify an object by selecting them in the list and clicking Remove or Edit (respectively).

The user's definition includes access permissions to and from specific machines at specific times of the day. The user definition can be used in the Rule Base's Authentication Rules and in Remote Access VPN.

SmartDashboard further facilitates user management by allowing you to define user and administrator templates. Templates serve as prototypes of standard users, whose properties are common to many users. Any user you create based on a template inherits all of the template's properties, including membership in groups.

Users Database
The users defined in SmartDashboard (as well as their authentication schemes and encryption keys) are saved to the proprietary Check Point Internal Users Database (the Users Databases) on the Security Management server.

The Users Database is automatically downloaded to Check Point hosts with installed Management Software Blades as part of the Policy installation process. Alternatively, you can manually install the Users Database by selecting Policy > Install Database... from the menu. Security Gateways that do not include a Management Software Blade do not receive the Users Database.
Managing Users in SmartDashboard

The Users Database does not contain information about users defined externally to the Security Management server (such as users in external SmartDirectory (LDAP) groups), but it does contain information about the external groups themselves (for example, on which Account Unit the external group is defined). For this reason, changes to external groups take effect only after the Security Policy is installed or after the Users Database is downloaded.

User and Administrator Types

SmartDashboard allows you to manage a variety of user and administrator types:

- **Administrators** — Login to a Check Point SmartConsole (SmartDashboard, SmartUpdate, etc.) with either Read Only or Read/Write permissions to view or manage (respectively) the network’s various databases and policies.

- **Administrator Groups** — Consist of administrators and of administrator sub-groups. Administrator Groups are used to specify which administrators have permissions to install Policies on a specific gateway.

- **External User Profiles** — Profiles of externally defined users, that is, users who are not defined in the internal users database or on an LDAP server. External user profiles are used to avoid the burden of maintaining multiple Users Databases, by defining a single, generic profile for all external users. External users are authenticated based on either their name or their domain.

- **Groups** — User groups consist of users and of user sub-groups. Including users in groups is required for performing a variety of operations, such as defining user access rules or RemoteAccess communities.

- **LDAP Groups** — An LDAP group specifies certain LDAP user characteristics. All LDAP users defined on the LDAP server that match these characteristics are included in the LDAP group. LDAP groups are required for performing a variety of operations, such as defining LDAP user access rules or LDAP RemoteAccess communities. For detailed information on LDAP Groups, see SmartDirectory (LDAP) and User Management (on page 115).

- **Templates** — User templates facilitate the user definition process and prevent mistakes, by allowing you to create a new user based on the appropriate template and change only a few relevant properties as needed.

- **Users** — Either local clients or remote clients, who access your network and its resources.

Configuring User Objects

This section describes how to configure standard user objects through the Users and Administrators tab of the Objects Tree (see the following figure). You can apply the same principles to configure other types of users (administrators, administrator groups, etc.).

**Figure 1-3**  
User Objects (Users, administrators, etc.) are defined in the Users and Administrators tab

**Configuring Users**

To configure user properties:

1. In the Users and Administrators tab of the Objects Tree, create a new user.
The User Properties window is displayed.

2. In the General tab, specify the User's Login Name.

   Note - If this user's certificate is to be generated by a non-Check Point Certificate Authority, the Login Name is the Common Name (CN) component of the user's Domain Name (DN).
   For example, if the user's DN is: [CN = James, O = My Organization, C = My Country],
   the user's Login Name is James.
   CNs used as Login Names must consist of a single string (with no spaces).

   This property is the user's only mandatory property and is case sensitive.

3. Define additional user properties as needed, such as the following:

   - The time period during which this user definition is valid.
   - The groups this user Belongs to (specified in the Groups tab).
     Including users in groups is required for performing a variety of operations, such as defining User Authentication rules or RemoteAccess communities.
   - The network objects from which (Source objects) and to which (Destination objects) the user is allowed access (specified in the Location tab).
   - The days and times during which the user is allowed to connect to the network (specified in the Time tab).
   - Authentication settings.
   - Certificate and encryption settings.

**Configuring Administrators**

1. In the Users and Administrators tab of the Objects Tree, create a new administrator.
   The Administrator Properties window is displayed.

2. In the General tab, specify the administrator's Login Name and Permissions Profile.

3. In the Admin Certificates tab, create a login certificate for this administrator as follows:
   a) Click Generate and save.
      You are warned that the certificate generation cannot be undone unless you click Revoke.
   b) Click OK.
      The Enter Password window is displayed.
   c) Enter and confirm the Password to be used with this certificate.
   d) Click OK.
      The Save Certificate File As window is displayed.
   e) Browse to the folder in which you wish to save the certificate and click Save (by default, the certificate is saved under the administrator's Login Name but you can rename it as needed).
      Back in the Admin Certificates tab, the Certificate State changes to Object has a certificate and the administrator's Distinguished Name (DN) is displayed.

4. Click OK.
   The administrator's definition is saved to the Users Database on the Security Management server.

**Configuring Templates**

To create a new user template:

1. In the Users and Administrators tab of the Objects Tree, create a new template.
   The User Template Properties window is displayed.

2. In the General tab, specify the template's name in the Login Name field.
   This property is mandatory and is case sensitive.

3. Define additional user properties as needed (see step 3 in Configuring Users (on page 25)).
To use this template to define a new user:
1. Right-click the Users folder and select New User > Template name...
2. In the General tab, specify the new user's Login Name. This is the only property the user cannot inherit from the template.
3. Choose one of the following:
   - To complete the user definition using the template's default settings, click OK.
   - To specify the user's unique properties, modify the relevant settings as needed and click OK.
   The template's definition is saved to the Users Database on the Security Management server.

Configuring Groups

To create a new user group:
1. In the Users and Administrators tab of the Objects Tree, create a new user group.
   The Group Properties window is displayed.
2. Specify the group's name in the Name field.
   This property is the group's only mandatory property and is case sensitive.
3. Move the users, external user profiles or groups to be included in this group from the Not in Group list to the In Group list.
   - To easily locate objects in the Not in Group list, limit the View to a specific type of objects (for example, users).
   - The In Group list shows collapsed sub-groups, without listing their members.
     For a list of all group members (including the sub-group’s members), click View Expanded Group...
4. Click OK to complete the definition.
   The group's definition is saved to the Users Database on the Security Management server.

Working with Policies

Overview

A Policy Package is a set of Policies that are enforced by the gateways. They can be installed or uninstalled together on selected Security Gateways. The Policy Package components include:

- **Advanced Security** — consisting of
  - the Firewall Rule Base
  - the Address Translation (NAT) Rule Base
  - the Users Database — the proprietary Check Point Internal User Database, containing the definitions and authentication schemes of all users defined in SmartDashboard.
  - the Objects Database — the proprietary Check Point Objects Database, containing the definitions of all network objects defined in SmartDashboard.

- **QoS** — the Quality of Service (Check Point QoS) Rule Base

- **Desktop Security** — the Desktop Security Rule Base

The installation process does the following:

1. Performs a heuristic verification on rules, to ensure they are consistent and that no rule is redundant. If there are verification errors (for example, when two of the Policy's rules are identical) the Policy is not installed. However, if there are verification warnings (for example, when anti-spoofing is not enabled for a gateway with multiple interfaces), the Policy Package is installed with a warning.
2. Confirms that each of the Gateways on which the rule is enforced (known as the Install On objects) enforces at least one of the rules. Install On objects that do not enforce any of the rules enforce the default rule, which rejects all communications.
3. Converts the Security Policy into an Inspection Script and compiles this Script to generate an Inspection Code.
4. Distributes the Inspection Code to the selected installation targets.
5. Distributes the User and Encryption databases to the selected installation targets.
To Install a Policy Package

To install a Policy Package:

1. Display the Policy package in the Rule Base.
2. Choose Policy > Install... from the menu.
   The Install Policy window is displayed.

   Note - The Policy to be installed includes implied rules, resulting from the Global Properties settings. To view the implied rules, select View > Implied Rules from the menu.

3. Choose the installation components:
   a) Installation Targets — the VPN gateways on which the Policy is installed. By default, all internal Gateways are available for selection. Alternatively, you define specific Gateways per Policy Package through the Select Installation Targets window (accessed by clicking Select Targets...).
   b) For each installation target, choose the Policy components (Advanced Security, QoS or Desktop Security) to be installed.
   c) The installation Mode — what to do if the installation is not successful for all targets (so different targets enforce different Policies):
      - Install on each gateway independently, or
      - Install on all gateways, or on none of the gateways

   Note - If you are installing the Policy on a gateway Cluster, specify if the installation must be successful for all Cluster Members.

4. Click OK.
   The Installation Process window is displayed, allowing you to monitor the progress of the verification, compilation and installation.
   If the verification is completed with no errors and the Security Management server is able to connect to the gateway securely, the Policy installation succeeds.
   If there are verification or installation errors, the installation fails (in which case you can view the errors to find the source of the problem).
   If there are verification warnings, the installation succeeds with the exception of the component specified in the warning.

   To find out which Policy is installed on each Gateway, select File > Installed Policies...

To Uninstall a Policy Package

To uninstall a Policy Package:

1. Display the Policy package in the Rule Base.
2. Choose Policy > Uninstall... from the menu.
   The Uninstall Policy window is displayed.

   Note - Uninstalling the Policy removes its implied rules as well.

3. Choose the Uninstall components.
4. Click OK.
   The Uninstall window is displayed, allowing you to monitor the progress of the operation. You are notified whether the uninstall has been completed successfully or has failed, and if so, for what reason.

Installing the User Database

The changes you make through SmartDashboard to user or administrator definitions are saved to the User Database on the Security Management server.
To provide your Check Point hosts with installed Management Software Blades with the latest user definitions, you must install the User Database on all relevant targets. Security Gateways that do not have an installed Management Software blade do not receive the User Database.

Choose one of the following options:

- **Policy > Install** — Choose this option if you have modified additional Policy Package components (for example, added new Security Policy rules) that are used by the installation targets.

- **Policy > Install Database** — Choose this option if the only changes you wish to implement are in the user or administrator definitions.
Chapter 2

Policy Management

In This Chapter

The Need for an Effective Policy Management Tool 30
The Check Point Solution for Managing Policies 30
Policy Management Considerations 34
Policy Management Configuration 34

The Need for an Effective Policy Management Tool

As corporate structures grow in size, more network resources, machines, servers, routers etc. are deployed. It stands to reason that as the Security Policy possesses more and more network objects and logical structures (representing these entities), used in an increasing number of rules, it becomes more complex and more of a challenge for the system administrator to manage.

Because of the complexity of the Security Policy, many system administrators operate according to the "if it ain't broke, don't fix it" axiom:

- New rules are often placed in a "safe" position (e.g. at the end of the Rule Base) rather than in the most effective position.
- Obsolete rules and objects are seldom eliminated.

These practices clutter and inflate the Security Policy and the databases unnecessarily, which invariably affects the performance of the Security Policy and the ability of the system administrator to manage it properly.

A simple, seamless solution is needed to facilitate the administration and management of the Security Policy by the system administrator. This easy-to-use policy management tool needs to take into account:

- The complexity of the corporate structure, with its multiple sites and branches, each of which has its own specific corporate needs.
- The need to easily locate objects of interest.
- The need to analyze the Rule Base.

The Check Point Solution for Managing Policies

Policy Management Overview

The Security Management server provides a wide range of tools that address the various policy management tasks, both at the definition stage and at the maintenance stage:

- *Policy Packages* allow you to easily group different types of Policies, to be installed together on the same installation target(s).
- *Predefined Installation Targets* allow you to associate each Policy Package with the appropriate set of gateways. This feature frees you of the need to repeat the gateway selection process every time you
install (or uninstall) the Package, with the option to easily modify the list at any given time. In addition, it minimizes the risk of installing policies on inappropriate targets.

- **Section Titles** allow you to visually break down your Rule Base into subjects, thereby instantly improving your orientation and ability to locate rules and objects of interest.

- **Queries** provide versatile search capabilities for both objects and the rules in which they are used.

- **Sorting** your objects in the Objects Tree and Objects List pane is a simple and quick way to locate objects. This feature is greatly facilitated by consistent use of naming and coloring conventions.

## Policy Packages

Policy Packages allow you to address the specific needs of your organization's different sites, by creating a specific Policy Package for each type of site. The following diagram illustrates an example organization's network, consisting of four sites.

**Figure 2-4** Example Organization with Different Types of Sites

Each of these sites uses a different set of Check Point Software Blades installed on the Security Gateways:

- **Servers Farm** has the firewall blade installed.
- **Sales Alaska** and **Sales California** sites have both the firewall and the VPN blades installed.
- **Executive Management** has the firewall, VPN and QoS blades installed.

Even sites that use the same product may have very different security needs, requiring different rules in their policies.

To manage these different types of sites efficiently, you need three different Policy Packages. Each Package should include a combination of policies that correspond to the products installed on the site in question.

Accordingly, a Policy Package is composed of one or more of the following policy types, each controlling a different Check Point blade:

- A Firewall and NAT Policy, controlling Security Gateways. This Policy also determines the VPN configuration mode.
- A QoS Policy, controlling Check Point QoS gateways.
- A Desktop Security Policy, controlling SecuRemote/SecureClient machines.

Unlike the above Policies, the Security Rule Base does not apply to a specific site but to the relationship between sites. Therefore, this Rule Base is common to all sites.

The Web Access Rule Base is independent of Policy Packages, since it applies to the organization as a whole (as opposed to a specific site). Its appearance in the Rule Base pane is determined by the Global Properties settings in SmartDashboard (see the SmartDashboard Customization page of the Global Properties window).
**File Operations**

File operations (New, Open, Save etc.) are performed at the Policy Package level (as opposed to the single policy level).

- **New** allows you to either define a new Policy Package, or add a single policy to an existing Policy Package.
- **Open** allows you to display an existing Policy Package. The policy types included in the Policy Package determine which tabs are displayed in the Rule Base.
- **Save** allows you to save the entire Policy Package.
- **Save As** allows you to save the entire Policy Package, or to save a specific policy that is currently in focus in the Rule Base (i.e. Security and Address Translation, QoS or Desktop Security).
- **Delete** allows you to delete the entire Policy Package.
- **Add to Policy Package** allows you to add existing Policies to your Policy Package.
- **Copy Policy to Package** allows you to copy existing Policies to your Policy Package.

**Note** - To back up a Policy Package before you modify it, use the Database Revision Control feature. Do not use File operations for backup or testing purposes, since they clutter the system with extraneous Packages. In addition, as there are multiple Packages but only one Objects Database, the saved Package may not correspond to changes in the Objects Databases.

**Installation Targets**

To install (and uninstall) Policy Packages correctly and eliminate errors, each Policy Package is associated with a set of appropriate installation targets. This association both eliminates the need to repeat the gateway selection process per installation, and ensures that Policy Package is not mistakenly installed on any inappropriate target.

The installation targets are defined for the whole Policy Package, thereby eliminating the need to specify them per-rule in each policy. The selected targets are automatically displayed every time you perform an Install or Uninstall operation.

**Figure 2-5** Example Installation Targets in the Install Policy window

You can set the Package's Policies to be either checked or unchecked by default for all installation targets (in the SmartDashboard customization page of the Global Properties window), and then modify these settings as needed per-installation.
Dividing the Rule Base into Sections using Section Titles

Section Titles enable you to visually group rules according to their subjects. For example, medium-size organizations may have a single policy for all of their sites, and use Section Titles to differentiate between the rules of each site (larger organizations with more complex Policies may prefer to use Policy Packages). Arranging rules in sections must not come at the expense of placing the most commonly matched rules at the beginning of the Rule Base.

Querying and Sorting Rules and Objects

Querying Rules

Querying rules can deepen your understanding of the policy and help you identify the most appropriate place for new rules. You can run queries on the Security, Desktop Security and Web Access Rule Bases.

A query consists of one or more clause statements. Each statement refers to the relationship between the selected object(s) and a specific column in the rule. You can apply the query to single objects, groups of objects or both. To further enhance the query, you can use the appropriate logical condition ("Negate", "And" or "Or").

Once you apply the query, only rules matching its criteria are displayed in the Rule Base. Rules that do not match the query are hidden, but remain an integral part of the policy and are included in its installation. You can refine these query results by running additional queries.

An example scenario in which Rule Base queries are useful is when a server running on host A is moved to host B. Such a change requires updating the access permissions of both hosts. To find the rules you need to change, you can run a query that searches for all rules where host A or host B appear in the Destination column.

By default, the query searches not only for rules that include these hosts, but also for rules that include networks or groups that contain them, as well as rules whose Destination is Any. Alternatively, you can search only for rules that explicitly include these objects.

Querying Network Objects

The Network Objects query allows you to find objects that match the query criteria. You can use this query tool to both control and troubleshoot object-related issues.

The query lists either All objects in your system (the default selection) or a specific type of object (e.g. firewall installed, QoS installed, Security Clusters etc.). You can refine this list using a variety of filters (e.g. Search by Name, Search by IP etc.) and use wildcards in the string you search for.

In addition to these basic searches, you can also perform more advanced queries for:

- objects whose IP address does not match their interface(s)
- duplicate IP addresses used by several objects
- objects that are not used

Note - Objects that are used by entities defined on an LDAP server are considered by the query as "not used".

You can further benefit from the query results by defining them as a group. For example, you may wish to create a group of all Mail Servers in your system and use this group in your Rule Base. If your naming convention is to include the word "Mail" in a Mail Server's name, you can easily find these objects by showing All network objects, choosing the Search by Name filter and entering the string "Mail". Then create a group out of the results and use it in the appropriate rule.

This group object is also available through other Check Point SmartConsoles. For example, if you are using the SmartReporter, you can include this group as the source of connections in the Email Activity report.

Sorting the Objects Tree and the Objects List Pane

The Objects Tree features a right-click Sort menu, allowing you to sort each tab by type (the default selection), name or color. This sort parameter applies to the Objects List pane as well. In addition, the Objects List pane can be sorted by clicking the relevant column's title.
Policy Management Considerations

Conventions

It is recommended to define a set of object naming and coloring conventions, which can significantly facilitate locating the object(s) you need. For example, if you use a prefix indicating the object's location (e.g. NYC_Mail_Server), you can easily group all objects by their location, by simply sorting the Object List pane's **Name** column. Similarly, you can implement a coloring convention that indicates which site an object belongs to, and then sort the relevant Object Tree's tab by color.

Policy Management Configuration

Policy Package

**Creating a New Policy Package**

1. Choose **File > New** from the menu.
   
   The **New Policy Package** window is displayed.

2. Enter the **New Policy Package name**. This name cannot:
   
   - Contain any reserved words, spaces, numbers at the beginning, or any of the following characters: %, #, $, &, @, ?, <, >, \, :
   - End with any of the following suffixes: .w, .pf, .W.

3. In the **Include the following Policy types** section, select any or all of the following policy types, to be included in the Policy Package:
   
   - Security and Address Translation
   - QoS — Traditional mode or Express mode
   - Desktop Security

   The table below lists the Rule Base tabs corresponding to each policy type.

   **Table 2-1 Rule Base tabs per Policy Type**

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Rule Base Tabs Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall and Address Translation</td>
<td>Firewall, NAT, IPS, Anti-Spam &amp; Mail, Anti-Virus &amp; URL Filtering, SSL VPN, and IPSec VPN</td>
</tr>
<tr>
<td>QoS</td>
<td>IPS, Anti-Spam &amp; Mail, Anti-Virus &amp; URL Filtering, SSL VPN, and QoS</td>
</tr>
<tr>
<td>Desktop Security</td>
<td>IPS, Anti-Spam &amp; Mail, Anti-Virus &amp; URL Filtering, SSL VPN, and Desktop</td>
</tr>
</tbody>
</table>

4. Click **OK** to create the Policy Package.
   
   SmartDashboard displays the new Policy Package, consisting of the selected policy type tabs.
Defining the Policy Package's Installation Targets

1. Choose Policy > Policy Package Installation Targets... from the menu. The Select Policy Package Installation Targets window is displayed.
2. Choose one of the following:
   - All internal modules (the default option)
   - Specific modules, selected by moving the relevant installation targets from the Not in Installation Targets list to the In Installation Targets list.
3. Click OK.
   The selected modules will be available as installation targets whenever you install or uninstall this Policy Package.
4. To set the default state of all modules to either Selected or Not Selected, thereby facilitating the policy installation (or uninstall) process, choose Policy > Global Properties and select the appropriate setting in the Global Properties window's SmartDashboard Customization page.
5. You can further modify the installation targets as part of the installation (or uninstall) operation:
   - To modify the targets of this operation only, check the relevant modules and Policies and uncheck all others.
   - To modify the targets of all future operations as well, click Select Targets... to display the Select Installation Targets window and modify the list as needed.

Adding a Policy to an Existing Policy Package

1. Choose File > Add Policy to Package... from the menu. The Add Policy to Package window appears.
2. Select one or more of the available policy types (for example, Security and Address Translation, Qos and Desktop Security).
3. Click OK.

Rule Sections

Adding a Section Title

1. Select the rule above which or under which you want to add a section title.
2. Choose Rules > Add Section Title > Above or Below (respectively) from the menu. The Header window is displayed.
3. Specify the title of the new section and click OK.
   The new section title is displayed in the appropriate location. All rules between this title and the next title (or the end of the Rule Base) are now visually grouped together.
4. By default, the section is expanded. To hide the section's rules, collapse its title by clicking the (-) sign.
5. If the rules following this section are not preceded by their own section title, you can mark the end of this section by adding an appropriate title (e.g. "End of Alaska Rules").

Querying the Rule Base

Configuring a New Query

1. Display the Rule Base you wish to query (Security, Desktop Security or Web Access) and select Search>Query Rules... from the menu. The Rule Base Query Clause / View Policy of Gateway window is displayed.
2. Select the Column you wish to query (e.g. Destination) from the drop-down list.
3. Move the object(s) to which your query applies from Not in List to In List.
4. If you have selected more than one object, specify whether it is enough for the selected column to contain at least one of these objects (the default option), or must it contain all of them.
5. This clause searches for rules where the specified column contains either the selected objects, or other objects they belong to (e.g. groups or networks).
• To search for rules where the specified column does not contain the selected objects, check Negate.
• To search only for rules where the specified column contains the objects themselves (as opposed to a group of network they belong to), check Explicit.

6. To run this query clause, click Apply. The rules matching the query clause are displayed in the Rule Base, while all other rules are hidden.

7. To save this query clause, click Save. The Save Query window is displayed.

8. Specify this query’s name and click OK. The Rule Base Queries window is displayed, showing the new query in the SmartDashboard Queries List.

Intersecting Queries

1. Display the Rule Base you wish to query (Security, Desktop Security or Web Access) and select Search>Manage Rule Queries from the menu. The Rule Base Queries window is displayed.

2. Select the first query you wish to run and click Apply. The rules matching this query are displayed in the Rule Base, while all other rules are hidden.

3. If you cannot find a relevant query on the list, you can define one now as follows:
   a) Click New...
      The Rule Base Query window is displayed.
   b) Specify the new query’s Name and click New...
      The Rule Base Query Clause / View Policy of Gateway window is displayed.
   c) Define the query (see Configuring a New Query (on page 35) - step 2 to step 5) and click OK. The query is added to the Clause list.
   d) You can add new clauses to the query and use the following logical operations:
      • And, to search for rules matching all clauses
      • Or, to search for rules matching at least one of the clauses
      • Negate query, to search for the negation of these clauses

4. Select the second query you wish to run.

5. Click one of the following:
   • And, so that only rules matching both queries are displayed
   • Or, to show rules that match either one of the queries

6. Run the selected query by clicking Apply.

7. To unhide all rules, click Clear all.

Querying and Sorting Objects

Querying Objects

1. Choose Search > Query Network Objects from the menu. The Network Objects window is displayed, showing All network objects in your system (the default selection) in the Network objects section. Alternatively, you can narrow down the display to the relevant object type (e.g. firewall installed, Check Point QoS installed etc.).

2. In the Refined Filter section, specify the appropriate search criterion, for example:
   • To find objects whose names contain a specific string, choose Search by Name from the Refine by drop-down list, enter the string you wish to search for (you may use wildcards) and click Apply.
   • To find objects with duplicate IP addresses, choose Duplicates from the Refine by drop-down list. The objects that match the search criteria are displayed.

3. To find one of these objects in SmartMap, click Show.
4. To create a group consisting of the search results, click Define query results as group... and specify the new group's name in the Group Properties window.

**Sorting Objects in the Objects List Pane**

1. Display the Object Tree's relevant tab (e.g. Services).
2. In the Objects List pane, click the relevant column's title (e.g. Port).
   You can now easily locate the object(s) in question. For example, you can find services that are using the same port.
Chapter 3

SmartMap

Overview of SmartMap

Most organizations have multiple gateways, hosts, networks and servers. The topology of these organizations is represented in SmartDashboard by network objects. The topology is often highly complex, distributed over many different machines and enforced in many different rules and rule bases. While this layout matches the needs of your organization, it is difficult to visualize, and even harder to translate in a schematic format. While the network objects are easy to use in the Rule Base, it would be easier to understand and troubleshoot the policy if the rules were displayed in a format where they could be understood visually.

The SmartMap Solution

SmartMap view is a visual representation of your network. This view is used to facilitate and enhance the understanding of the physical deployment and organization of your network.

SmartMap is used in order to:

- Convert the logical layout of your organization into a graphical schematic layout which can be exported as an image file, or printed out.
- Show selected network objects, communities and rules within the graphical representation, by right-clicking on these items from numerous places in the various Rule Bases, Object Tree pages and Object List. For enhanced visualization you can zoom into these selected items.
- Edit objects displayed in SmartMap. The changes made will be integrated throughout SmartDashboard.
- Troubleshoot the policy. For instance SmartMap can resolve unresolved objects, and it can make automatic calculations for objects behind the gateway, Install On targets and for anti-spoofing purposes.

Working with SmartMap

Enabling and Viewing SmartMap

Before you begin to work with SmartMap you need to enable it. In this section you can learn how to enable, toggle and launch SmartMap.

Enable SmartMap

It is not possible to work with SmartMap until it has been enabled.

- To enable SmartMap go to Policy > Global Properties > SmartMap.
Toggle SmartMap

In order to clear SmartDashboard of visual clutter, SmartMap can be toggled until such time that you need to work with it again.

Note - When the SmartMap view is hidden or inactive, all of its menus and commands are disabled; however, topology calculations do continue.

- To view SmartMap go to View > SmartMap.
- To disable SmartMap go to View > SmartMap.

Launching SmartMap

SmartMap can be displayed, embedded or docked into the GUI window, or it can be displayed outside of the SmartDashboard window.

- To display SmartMap outside the SmartDashboard window, go to SmartMap > Docked View.

Adjusting and Customizing SmartMap

All of the following options affect the way that SmartMap is viewed or displayed.

Magnifying and Diminishing the SmartMap View

The level of magnification can be selected or customized. The operations that can be executed include:

- enhancing the view so that all or a selected part of SmartMap optimally fits into the display window.
- selecting from one of the displayed zoom values or customizing your own (for example, Zoom In (magnify) or Zoom Out (diminish) the current SmartMap display).
- magnifying an area in SmartMap by dragging the mouse over a specific area. All objects that fall within the area of the selected box will be magnified.

To automatically zoom into a particular area of SmartMap:

1. Select SmartMap > Zoom Mode.
2. Drag the mouse over a specific area in SmartMap.
   The area you selected will zoom into view.

To select the level of magnification

1. Select SmartMap > Select Mode.
2. Drag the mouse over a specific area in SmartMap.
3. Select SmartMap > Zoom > sub menu and select the options that best meet your needs.

Scrolling

If you have an IntelliMouse you can use the scroll wheel to scroll SmartMap.

Adjusting SmartMap using the Navigator

The Navigator is a secondary window that displays an overview of SmartMap. This view can be adjusted by altering the select box. As parts of SmartMap are selected in the Navigator window, the SmartMap display is altered to match the selected area. When the Navigator window is closed, its coordinates are saved and when it is reopened, the same view of SmartMap is displayed.

- To launch the Navigator, go to SmartMap > View Navigator.

Affecting SmartMap Layout (Arranging Styles)

SmartMap enables you to determine the manner in which network objects are placed within SmartMap in one of two possible styles.

- To select a SmartMap style, go to SmartMap > Customization > Arranging Styles and select one of the following:
  - hierarchic — SmartMap resembles a tree graph
• **symmetric** — SmartMap resembles star and ring structures

**Optimally arranging SmartMap (Global Arrange)**

Use **Global Arrange** to optimally arrange the whole SmartMap within the entire view. SmartMap will be arranged according to the currently set arrange style.

- To arrange the entire SmartMap, go to **SmartMap > Arrange > Global Arrange**.

**Optimally arranging SmartMap (Incremental Arrange)**

Use **Incremental Arrange** to optimally arrange a selected area of SmartMap within the entire view. SmartMap will be arranged according to the currently set arrange style.

- To arrange a selected area, go to **SmartMap > Arrange > SmartMap > Arrange > Incremental Arrange**.

**Working with Network Objects and Groups in SmartMap**

Network Objects are represented by standardized icons in SmartMap. Network Object icons are connected by edges. Edges (also called connections) are the lines or links that are drawn automatically or manually between network objects in SmartMap. These connections can be fixed or they can be editable.

In order to work with objects, you need to be in **SmartMap > Select Mode**, this mode is the default working mode that allows you to select the object in SmartMap.

SmartMap can be used to add and edit network objects. All items in SmartDashboard that are representations of physical network objects, (such as OSE Devices and network objects), can also be seen and edited in the SmartMap view. Objects that are not representations of physical network objects, (such as Address ranges), cannot be seen in SmartMap.

**Add a Network Object to SmartMap**

1. Right-click in SmartMap and select **New Network Object** from the displayed menu.
2. Select the object that you would like to add. The Object's Properties window is displayed. Configure the new object.

   **Note** - You can add a new network object directly to a network. Right-click on a specific network in SmartMap and then continue according to the previous instructions.

**Create a Group**

1. Select all the objects that you would like to include in the group.
2. Right-click on the selected objects and select **Group** from the displayed menu.
3. Configure the group by adding or removing objects to and from the group.

**Edit Network Objects**

1. Do one of the following
   - Double-click on an object in SmartMap, or
   - Right-click on a selected object in SmartMap and select **Edit** from the displayed menu.
2. Edit the object. Note that if you change the IP address of a selected object, the placement of the object in SmartMap may change accordingly.

**Remove Network Objects**

1. Right-click on the selected object(s) that you would like to delete.
2. Select **Remove** from the displayed menu. You are prompted to make sure that you would like to remove the selected object(s)
3. Click **Yes** to continue.
Note - A warning will be displayed if you attempt to remove an object that is used in the policy. If you ignore the warning the object will still be removed and SmartMap will be adjusted accordingly.

**Fixed Connections versus Editable Connections**

- **Automatic connections** — these are non-editable connections that exist between objects whose topology can be deterministically calculated. These connections can only be changed if the objects connected by them are edited. A non-editable connection can be made into an editable one, if other objects are added or modified. For example, if a host is uniquely connected to a network and later an identical network is defined, the host's connection will be changed from a fixed connection to an editable one to allow for the host to be moved from the one network to the other.

- **Editable connections** — these are editable connections that can be created automatically by SmartMap by adding or modifying objects (for instance by modifying the connection between contained and containing networks), or they can be manually defined by the user. For example, when ambiguous networks are resolved, or when networks are connected to the Internet or to other networks (either by a containment relation or using a connectivity cloud), these connections can be disconnected by right-clicking on the connecting UTM-1 Edge and selecting **Disconnect**.

**Select an area in SmartMap (Select Mode)**

Select an area in SmartMap by dragging the mouse over a specific area. All objects that fall within the area of the select box will be selected. Objects that are selected in Select Mode can be dragged to another area in SmartMap.

To move to **Select Mode**, go to **SmartMap > Select Mode**.

**Customize color and width of objects and edges**

Only the width of edges can be customized.

To change options, go to **SmartMap > Customization > View Options**.

**Setting the Layers for SmartMap**

Not all object types can be viewed automatically in SmartMap. You can decide what types of layers you would like to add to your view. You can select from the basic layer which provides you all default objects, and from the OPSEC layer which adds certain OPSEC object types.

To set layers, go to **SmartMap > Customization > View Options**.

**Customize Tooltips for Objects**

Select the Information about the network object to be displayed when the cursor passes over the object in SmartMap.

To customize tooltip information, go to **SmartMap > Customization > Tooltips Information**.

**Customize the Display of Object Labels and IP Addresses**

Select Object Label and IP Address attributes and limitations.

To customize, go to **SmartMap > Customization > Object Label Options**.

**Working with SmartMap Objects**

SmartMap maintains graphic connectivity between different parts of the network by creating and adding several new topology objects, such as:

- **Internet Objects** — represents the Internet.
- **Connectivity Clouds** — represents a private web or an Intranet.
• **Implied Networks** — a network that is created when a created network object has no viable network to which it can be connected. This network is read-only and non-editable although it can be *actualized*, that is, made into a real network.

• **Ambiguous Networks** — a network that is created when a created network object has multiple viable networks to which it can be connected. The network object is connected to the ambiguous network and the user must decide to which network the network object should be connected.

  📝 *Note* - Topology objects, or objects created by the SmartMap view, such as clouds and implied networks, etc., cannot be defined as protected objects. They cannot be included in any group, nor can they be pasted into the SmartDashboard Rule Base.

• **Contained Networks** — A Contained Network is always derived from the same or lower net mask class as the Containing Network.

### Add an Internet Cloud

The Internet Cloud defines connectivity between the network object and a public network without supplying technical details of the path between them. Multiple Internet clouds can be added to SmartMap. These clouds are non-editable. When SmartMap performs calculations it looks for Internet clouds and uses them to identify whether interfaces are external or internal.

To create a new cloud, go to **SmartMap > New Internet Cloud**.

### Add a Connectivity Cloud

The Connectivity Cloud defines connectivity between the network object and a private network without supplying technical details of the path between them. Multiple Connectivity clouds can be added to SmartMap. These clouds are editable.

To add a connectivity cloud, go to **SmartMap > New Connectivity Cloud**.

### Connecting a Network to Internet Clouds

There is always at least one Internet cloud in SmartMap. This cloud cannot be deleted. A line is automatically drawn between an existing network and the sole Internet cloud.

### Connecting a network to Connectivity clouds/an Internet cloud, where there is more than one/a Containing Network

1. Right-click on the network you would like to connect to the Connectivity cloud by holding down the `ctrl` key until all networks are selected.
2. Right-click the last selected network.
3. Select `Connect to` and select the option that you would like.

### Connecting multiple networks to a Connectivity Cloud

Since SmartMap connects networks according to their IP addresses hierarchy, contained networks are automatically connected to their parent network. This connection is editable and can be removed.

1. Select the networks that you would like to connect to the Connectivity cloud.
2. Select **Connect Networks**.
3. Specify the Connectivity cloud settings.

### Viewing the Settings of an Implied network

The Implied network is named by its IP address and a superimposed "I". It is Read Only, unless it is *actualized*, or made into a real network.

1. Right-click the Implied Network.
2. Select **View** from the displayed menu.

### Actualizing an Implied network

The Implied network is Read Only, unless it is *actualized*, or made into a real network. This means that it is made into a functioning network with its own specification and legitimate (legal or illegal) IP address.
1. Right-click the Implied network.
2. Select Actualize from the displayed menu.
3. Configure the settings.

Removing the Connection between a Containing and a Contained network
1. Right-click the UTM-1 Edge of the Contained Network.
2. Select Disconnect from the displayed menu.

Working with Folders in SmartMap

Topology collapsing, often referred to as folding, facilitates the use of SmartMap by expanding or collapsing topology structures. This collapsing mechanism simplifies SmartMap, by ridding it of visual clutter, but still preserving its underlying structure. The folding mechanism allows you to collapse certain topology structure types. The folders can be created at the following points:

- On a UTM-1 Edge that is an interface as well as all the objects behind it.
- On any network which has hosts or containing networks.
- On any gateway and its locales.

There are two special folders which can be collapsed:

- **Objects To Resolve** — contains network objects and unresolved hosts that are ambiguous.
- **External Objects** — contains hosts which have no networks to which they can be connected (because they do not fit into any network's IP address range) as well as any standalone networks. This folder does not include Check Point installed objects.

Collapsing locales

1. Right-click the locale.
2. Select Collapse Locale from the displayed menu.

Collapsing other Topology Structures

1. Right-click on the object that you would like to collapse.
2. Select Collapse Object where object is a variable depending on the object that you selected.

Expanding Topology folders

1. Right-click the folder which contains the content that you would like to view.
2. Select Expand from the displayed menu.

Viewing the Content of "special" folders

**External Objects** and **Unresolved Objects** are two special types of folders which cannot be expanded, but whose contents can be viewed:

1. Right-click the folder whose contents you would like to view.
2. Select Show Contents from the displayed menu.

Hiding the contents of "special" folders

**External Objects** and **Unresolved Objects** are two special types of folders which cannot be expanded, but whose contents can be hidden:

1. Right-click the folder whose contents you would like to hide.
2. Select Hide Contents from the displayed menu.

Defining the contents of a "special" folder as a group

1. Right-click the folder whose member you would like to group.
2. Select Define as Group from the displayed menu.
3. Configure the Group Properties window.
Renaming Topology folders

Folders are given a default name. This name can be edited.

1. Right-click the folder that you would like to rename.
2. Select Rename from the displayed menu.
3. Enter a new name for the folder.

Adding the contents of a SmartMap folder to the Rule Base

When the contents of the folder are dragged and copied into the Rule Base you will be prompted to decide whether or not to save the members of the folder as a group, or to add the contents member by member.

1. Select the folder whose contents you would like to add to the Rule Base.
2. Press the Shift key.
3. Drag the selected folder to the desired location in the Rule Base.
4. If the contents are added as a group, configure the Group Properties window.

Editing External Objects

External Objects are hosts which have no viable networks to which they can be connected. That is to say their IP address is not within the range of the IP address of any currently defined network.

1. Right-click the External Objects folder.
2. Select Edit from the displayed menu.
3. Configure the Properties window of the selected external object.

Viewing Gateway Clusters

The gateway cluster objects are never included in the Objects to Resolve folder, even though they may be unresolved.

1. Right-click the selected gateway cluster.
2. Select Show Members from the displayed menu.

Integrating SmartMap and the Rule Base

You can drag rules from the Rule Base and show them in SmartMap. You can enhance your understanding of the displayed rule by adding a Legend. You can paste objects and folders from SmartMap. You can show network objects selected in the Rule Base and some other locations in SmartMap.

Display a Legend for regular and/or NAT rules

The Legend provides a key to the understanding of rules displayed in SmartMap.

- To display a legend, go to SmartMap > Customization > View Options.

Adding the contents of a SmartMap folder to the Rule Base

See Working with Folders in SmartMap (on page 43).

Pasting Network Objects in the Rule Base

Topology objects (for instance clouds, ambiguous networks, etc.) cannot be pasted into the Rule Base.

1. Right-click on a selected network object.
2. Select Copy to Rule Base from the displayed menu.
3. Right-click the column in which the selected network object should be pasted.
4. Select Paste from the displayed menu.

Viewing a Network Object selected in the Rule Base in SmartMap

1. Select the Network Object in the Rule Base that you would like to show in SmartMap.
2. Drag the network object using the left mouse button, and drop it into SmartMap.
Viewing Network Objects selected in SmartMap in the Rule Base
1. Select the Network Object in SmartMap that you would like to show in the Rule Base.
2. Drag the network object using the left mouse button and the shift and alt buttons of the keyboard, and drop it into SmartMap.

Showing a rule in SmartMap
A rule that you select to show in SmartMap can be shown in a magnified view or according to the current zoom level.

Note - Only Security Policy rules can be shown in SmartMap View.

1. Select a rule in the Rule Base that you would like to display in SmartMap from the rule number.
2. Select Show and a view option from the displayed menu.

Display the Rule Color Legend
Rules appear as combinations of highlighted colors and arrows on SmartMap. For instance, colors are designated to represent the Source, Destination and Install On columns of SmartDashboard. These colors can be viewed in the Rule Color Legend window, which is displayed when a rule is shown.

Drag a rule into SmartMap and the Rule Color Legend is automatically displayed.

Understanding the Rule Color Legend
Rules appear as combinations of highlighted colors and arrows on SmartMap. The colors assigned to the arrows represent the action being performed. The arrow also indicates the direction of the rule; from whence the rule came (source), and to where it is going (destination).

- Red — Drop, Reject
- Green — Accept
- Blue — User Auth, Client Auth, Session Auth
- Purple — Encrypt, Client Encrypt

Rules that require special attention
When rules are shown in SmartMap, the "Any" value is represented by the icon • at the base or the head of the arrow, to indicate that the Source or Destination, respectively, is Any.

The rules mentioned below are mapped and displayed in a specific manner:

- Where the Source is Any, the rule is mapped from the Install On to the Destination.
- Where the Destination is Any, the rule is mapped out from the Source to the Install On.
- Where both Source and Destination are Any, only the paths between the Install Ons are shown.

Troubleshooting with SmartMap
SmartMap can be used as a troubleshooting tool, mostly for topology calculations and certain connectivity issues such as duplicated networks and unresolved object interfaces.

For what objects are topology calculations made?
Topology information specifies data about the object interfaces and the IP addresses behind the interfaces.

- Security Gateways with two or more interfaces
- OSE Devices

Calculating topology information
You can calculate topology for objects selected in the following places:

- SmartMap
- Objects Tree
• Objects List

The Legend in the Topology Calculation Results window explains how you are meant to read the Interfaces topology list.

• Red— the results of the calculation are different from the currently defined topology information. This information needs to be approved. Click Approve to display and contrast the current topology information with the resulting topology information. Click Approve all to automatically approve all calculations without comparing and contrasting results.

• Blue— the calculation has been automatically approved.

• Regular— no change has been made to the topology information.

To calculate topology for a selected object
1. Right-click the selected object.
2. Select Calculate Topology from the displayed menu.
3. The Topology Calculation Results window displays the topology information after a calculation has been made for the selected object.

What is SmartMap Helper?
SmartMap Helper teaches you how to solve tasks relating to connectivity such as:
• Duplicated networks
• Unresolved object interfaces

The Helper is a learning tool. Once you understand how to solve these connectivity tasks, you can solve them directly in SmartMap View, and not via the Helper.

Troubleshooting duplicated networks
Duplicated networks occur if there is more than one network with an identical net mask and IP address.

Note - Some network systems may require duplicated networks. Consider the needs of your system before modifying duplicated networks.

To solve duplicated networks you can modify the shared IP address so that they are all unique. Alternately you can delete the duplicated network.

Troubleshooting unresolved object interfaces
When there is more than one viable network to which a network object can be connected, the network object is temporarily connected to an Ambiguous network until such time that it can be properly resolved. See Ambiguous Networks in Working with SmartMap Objects (on page 41).

What objects can be defined as protected objects?
Any object which does not lead to the Internet can be defined as a protected object. This includes:
• Gateway clusters
• Security Gateways with two or more interfaces
• OSE Devices

Defining Protected Objects as Groups
Any object which does not lead to the Internet can be defined as a protected object group.
1. Right-click the selected object(s).
2. Select Define Protected Objects as Group from the displayed menu.
3. Configure the Group Properties window.
Working with SmartMap Output

Once you have set up your deployment there are several operations that can be performed. Make sure that you save and/or install your policy in order to ensure that all the changes made in SmartMap are applied. SmartMap is always displayed in the layout and with the last coordinates that it had when it was last saved. Once SmartMap is saved you can print SmartMap or even export it to another format for ease of use.

The following options are accessible from the SmartMap menu in SmartDashboard:

Print SmartMap

Set the attributes by which SmartMap will be printed. This includes how the output is to be scaled, the size of the margins and finally information to be included (such as page numbers, borders, crop marks, or even a customized caption).

Export SmartMap (as an image file)

Configure the attributes for images that are exported to an image file. Include the type and size of the image. Specify the treatment of folders in the exported image. Specify general information, including name, label, the date of export as well as a logical prefix that can be referred to and understood. This is especially important when saving multiple image files. Finally specify the location to which the image file will be saved and whether you want to open or to print the image files once they have been exported.

Export SmartMap (to Microsoft Visio)

You can configure the settings for SmartMap exported to Microsoft Visio. Specify object data that you would like to include. This includes general information about the object such as name, IP address and net mask. Specify the treatment of folders and icons during the export operation. You can preserve the Check Point icons and colors or you can choose to use icons from the Microsoft Visio stencil. Finally, decide which general information should be included on the output, for instance, the date, a label and the location to which the exported SmartMap will be saved.
Chapter 4

The Internal Certificate Authority

In This Chapter

The Need for the ICA 48
The ICA Solution 48
ICA Configuration 53

The Need for the ICA

The security needs of the customer are always foremost in Check Point software. Strong authentication is required and this authentication must comply with international security standards in order to ensure the secure connections of:

- Secure Internal Communication (SIC) – the feature which ensures strong authentication between internal Check Point entities
- VPN – for both gateways and users

The ICA Solution

Introduction to the ICA

The ICA is a Certificate Authority which is an integral part of the Check Point product suite. It is fully compliant with X.509 standards for both certificates and CRLs. See the relevant X.509 and PKI documentation, as well as RFC 2459 standards for more information. You can read more about Check Point and PKI in the R71 Virtual Private Networks Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10320).

The ICA is located on the Security Management server. It is created during the installation process, when the Security Management server is configured.

The ICA issues certificates for:

- SIC – certificates are issued for the Security Management server, its gateways, OPSEC modules, and product administrators in order to enable secure communication for all Check Point-related operations (such as policy installation on gateways, logging, SmartConsole-Security Management server connectivity, etc.).
- VPN certificates for gateways – to enable efficient and seamless strong authentication in VPN tunnel creation.
- Users – to enable strong authentication between remote access users and gateways, as well as other features, such as clientless VPN Security Management server.

The ICA issues Certificate Revocation Lists (CRLs) in order to publish a list of certificates that have been revoked. This revocation may be due to a number of factors: key compromise, certificate loss, etc. The CRLs are published on an HTTP server running on the Security Management server, and can be retrieved by any Check Point gateway for certificate validation.

ICA Clients

ICA operations are performed using the following clients:
Check Point configuration tool or cpconfig on the Command Line. Using this tool, the ICA is created and a SIC certificate is issued for the Security Management server. For more information, see Securing Channels of Communication (SIC) (on page 20).

SmartDashboard. This SmartConsole is used to manage:
- SIC certificates for the various gateways, as well as for administrators. For more information see Securing Channels of Communication (SIC) (on page 20).
- VPN certificates
- ICA Management tool. This tool is used to manage VPN certificates for users that are either managed on the internal database or on a LDAP server. Additionally it is used to perform ICA management operations.

The ICA generates audit logs when ICA operations are performed. These logs can be viewed in the SmartView Tracker.

Certificate Longevity and Statuses

Each certificate issued by the ICA has a defined validity period. When this validity period is over, the certificate becomes expired.

An administrator can revoke a certificate. This may be done for a number of reasons, for instance, when a user leaves the organization. If a certificate is revoked, the serial number of the certificate is published on the CRL indicating that the certificate has been officially revoked, and cannot be used or recognized by any entity in the system.

Certificates are created in different stages. SIC certificates, VPN certificates for gateways and User certificates are created in one step via SmartDashboard, although the latter can also be created in a two step process using either SmartDashboard or the ICA Management Tool. If the User certificate is created in two steps, these steps include:
- Initialization – during this stage a registration code is created for the user. When this is done, the certificate state is pending
- Registration – when the user completes the registration process in the remote client (SecuRemote/SecureClient) using the registration code the certificate becomes valid

The advantages of the two-step process are as follows:

Enhanced security
- the private key is created and stored on the user's machine
- the certificate issued by the ICA is downloaded securely to the client machine (and not handed to the user by the administrator)

Pre-issuance automatic and administrator-initiated certificate removal
If a user does not complete the registration process within a given period of time (which is by default two weeks), the registration code is automatically removed. An administrator can remove the registration key before the user completes the registration process. After that, the administrator can revoke the user certificate.

Explicit or Automatic Renewal of User certificates ensuring continuous User connectivity
A user certificate of type PKCS12 can be renewed explicitly by the user or it can be set to be renewed automatically when it is about to expire. This renewal operation ensures that the user can continuously connect to the organization's network. The administrator can choose when to set the automatic revocation of the old user certificate.

Another added advantage is:

Automatic renewal of SIC certificates ensuring continuous SIC connectivity
SIC certificates are renewed automatically after 75% of the validity time of the certificate has passed. If, for example, the SIC certificate is valid for five years, 3.75 years after it was issued, a new certificate is created and downloaded automatically to the SIC entity. This automatic renewal ensures that the SIC connectivity of the gateway is continuous. The administrator can decide to revoke the old certificate automatically or after a
set period of time. By default, the old certificate is revoked one week after the certificate renewal has taken place.

**SIC Certificate Management**

SIC certificates are managed in the **Communication** window of the gateway object.

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Default</th>
<th>Configurable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>validity</td>
<td>5 years</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>key size</td>
<td>1024 bits</td>
<td>yes</td>
<td>Can be set to 2048 or 4096 bits</td>
</tr>
<tr>
<td>KeyUsage</td>
<td>5</td>
<td>yes</td>
<td>Digital Signature and Key encipherment</td>
</tr>
</tbody>
</table>

All the attributes in the previous table can be set in the ICA Management Tool.

**Gateway VPN Certificate Management**

VPN certificates for gateways are managed in the **VPN** tab of the corresponding network object.

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Default</th>
<th>Configurable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>validity</td>
<td>5 years</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>key size</td>
<td>1024 bits</td>
<td>yes</td>
<td>Can be set to 2048 or 4096 bits</td>
</tr>
<tr>
<td>KeyUsage</td>
<td>5</td>
<td>yes</td>
<td>Digital Signature and Key encipherment</td>
</tr>
<tr>
<td>ExtendedKeyUsage</td>
<td>0 (no KeyUsage)</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

All the attributes in the previous table can be set in the ICA Management Tool.

**Note** - If the gateway certificate is stored on a hardware token, the key size is configured in the `Objects_5_0.C` file using the `dbedit` utility, see Modifying the Key Size (on page 51).

**User Certificate Management**

Internally managed User Certificates can be managed (for example, operations such as initialization, revocation or the removal of registrations can be performed) either from the **User Properties** window in SmartDashboard or by using the ICA Management Tool.

User Certificates of users who are managed on an LDAP server can only be managed via the ICA Management Tool.

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Default</th>
<th>Configurable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>validity</td>
<td>2 years</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>key size</td>
<td>1024 bits</td>
<td>yes</td>
<td>Can be set to 2048 or 4096 bits</td>
</tr>
<tr>
<td>Attributes</td>
<td>Default</td>
<td>Configurable</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>DN of User certificates managed by the internal database</td>
<td>CN=user name, OU=users</td>
<td>no</td>
<td>This DN is appended to the DN of the ICA</td>
</tr>
<tr>
<td>DN of User certificates managed on an LDAP server</td>
<td></td>
<td>yes</td>
<td>Depends on LDAP branch</td>
</tr>
<tr>
<td>KeyUsage</td>
<td>5</td>
<td>yes</td>
<td>Digital signature and Key encipherment</td>
</tr>
<tr>
<td>ExtendedKeyUsage</td>
<td>0 (no KeyUsage)</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

All the operations in the previous table can be performed via the ICA Management Tool.

**Modifying the Key Size**

If the user completes the registration from the Remote Access machine, the key size can be configured in the Advanced Configuration page in SmartDashboard. This page can be accessed by selecting Policy > Global Properties > SmartDashboard Customization > Advanced. This is the recommended method.

Alternately you can edit the key size using the `dbedit` utility of the Objects_5_0.C by modifying the size of the key as it is listed in `users_certs_key_size` Global Property. The new value is downloaded when the user updates his site.

**How is it done?**

In SmartDashboard or in the `dbedit` utility:

1. Change the attribute `ica_key_size` to one of the following values: 1024, 2048 or 4096.
2. Run `fwm sic_reset`.
3. Run `cpconfig` and define the CA name in the Certificate Authority tab.
4. When you are done, click OK.
5. Run `cpstart`.

**CRL Management**

By default, the CRL is valid for one week. This value can be configured. Fresh CRLs are issued:

- when approximately 60% of the CRL validity period has passed
- immediately following the revocation of a certificate

It is possible to recreate a specified CRL via the ICA Management Tool. This acts as a recovery mechanism in the event that the CRL is deleted or corrupted. Moreover, an administrator can download a DER encoded version of the CRL using the ICA Management Tool.

**CRL Modes**

The ICA is able to issue multiple CRLs. The purpose of multiple CRLs is to eliminate any CRL from becoming larger than 10K. If the CRL exceeds 10K, IKE negotiations may fail when trying to establish VPN tunnels.

Multiple CRLs are achieved by attributing every certificate which is issued to a specific CRL. If revoked, the serial number of the certificate appears in this specific CRL.

The CRL Distribution Point (CRLDP) extension of the certificate contains the URL of the specific CRL. This ensures that the correct CRL is retrieved when the certificate is validated.
ICA Advanced Options

Modifying the ICA Key

The ICA is created with a key of size 2048 bits. There are certain cases in which a key of a different size is required (of either 1024 or 4096 bits). In such a case, the ICA must be re-created. This can be done using the command lines and the ICA Configuration file.

The ICA Management Tool

The ICA Management Tool is a user-friendly tool that allows an administrator to perform multiple operations on and for the ICA, such as:

- Certificate management and searches
- CRL recreation and download
- ICA configuration
- ICA cleanup resulting in the removal of expired certificates

Note - The ICA Management Tool is supported by SSL version 3 and TLS.

The ICA Management Tool GUI

The Interface is divided into three panes:

- The Menu pane - select the operation to be performed from the menu pane.
- The Operations pane - the operation is configured and applied in this pane. From this window you can:
  - Manage Certificates - this window is divided into search attributes configuration and bulk operation configuration.
  - Create Certificates - from this window you can create certificates.
  - Configure the CA - this window contains the configuration parameters and enables the administrator to configure them. You can also view the CA's time, name, and the version and build number of the Security Management server.
  - Manage CRLs - from this window you can download, publish, or recreate CRLs.
- The Search Results pane - the results of the applied operation are displayed in this pane. This window consists of a table with a list of searched certificates attributes.

The ICA Management Tool is operational from any browser on any platform. Using HTTPS it is possible to connect securely from the ICA Management Tool to the ICA provided that an administrator certificate is added to the browser.

Note - The ICA Management Tool can connect to the ICA in clear, however for the sake of security it is recommended to work encrypted in HTTPS.

Notifying Users about Certificate Initialization

The ICA Management Tool can be used to send mail to users to notify them about certificate initialization. In order to send mail notifications, the administrator must configure:

1. the mail server.
2. the mail "From" address.
3. an optional "To" address, which can be used if the users' address is not known. In this case, when the certificates are issued, the administrator can get the mails and forward them to the corresponding address.
Performing Multiple Simultaneous Operations

In order to ease the management of user certificates the ICA Management Tool can perform multiple simultaneous operations. For example, it is possible to:

1. Make a single LDAP query for getting the details of all the organization employees.
2. Create a file out of this data, and then use this file to:
   - initiate the creation of certificates for all employees
   - notify all employees of these new certificates

The following are the types of operations that can be performed simultaneously:

- initiate user certificates
- revoke user certificates
- send mail to users
- remove expired certificates
- remove certificates for which the registration process was not completed

ICA Administrators with Reduced Privileges

The ICA Management Tool supports administrators with reduced privileges. These administrators can make basic searches and initialize certificates for new users. Multiple concurrent operations cannot be executed by these administrators. These administrators may typically be help desk operators who are charged with the handling of new employees.

ICA Configuration

Retrieving the ICA Certificate

In certain scenarios it is required to obtain the ICA certificate. Peer gateways that are not managed by the Security Management server need to use it for Trust purposes. Also, clients using Clientless VPN, as well as the machine on which the ICA Management Tool is run, require this certificate. In this case, these peers are requested to proceed as follows:

1. Open a browser and enter the appropriate URL (in the format http://<smart_dns_name>:18264)

   The Certificate Services window is displayed.

   Figure 4-6  Certificate Services window

   ![Certificate Services](Image)

   - [Install this CA certification path](#) to allow your computer to trust this CA certificates.
   - [Download CA certificate](#) to save this certificate on disk

2. In the Certificate Services window, you can download a CA certificate to your computer or in Windows you can install the CA certification path.

Management of SIC Certificates

SIC certificates are managed using SmartDashboard, for more information, see Securing Channels of Communication (SIC) (on page 20).
Management of Gateway VPN Certificates

VPN Certificates are managed in the VPN page of the corresponding network object. These certificates are issued automatically when the IPSec VPN blade is defined for the Check Point gateway or host. This definition is specified in the General Properties window of the corresponding network object, as shown below:

![Figure 4-7](image)

If this certificate is revoked, a new one is issued automatically.

Management of User Certificates via SmartDashboard

The User certificates of users that are managed on the internal database are managed using SmartDashboard. For more information, see the Remote Access VPN chapter in the R71 Virtual Private Networks Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10320).

Invoking the ICA Management Tool

The ICA Management Tool is disabled by default, and can be enabled via the command line.

1. Enable or disable the ICA Management tool using the command line on the Security Management server.

   Usage
   
   ```
   cpca_client [-d] set_mgmnt_tool on|off [-p <ca_port>] [-no_ssl] [-a|-u "administrator|user DN" ... ]
   ```

   where:
   - on means to start the ICA Management Tool (by opening port 18265)
   - off means to stop the ICA Management Tool (by closing port 18265)
-p changes the port used to connect to the CA (if the default port is not being used)
-no_ssl configures the server to use clear HTTP rather than HTTPS
-a "administrator DN" ... sets the DNs of the administrators that will be allowed to use the ICA Management Tool
-u "user DN" ... sets the DNs of the users that will be allowed to use the ICA Management Tool. This option is intended for administrators with limited privileges.

Note - If caca_client is run without -a or -u, the list of the allowed users and administrators will not be changed and the server will be started/stopped with the previously allowed users/administrators.

2. In order to connect to the ICA, add the administrator's certificate to the browser's certificate repository.
3. Open the ICA Management tool from the browser.

Open the browser and type the location: https://<Management_Host_Name>:18265
You will be requested to authenticate.

Note - The ICA Management Tool should not be on the same subnet as the Security Management server.

Search for a Certificate

Initiating a Search

This is performed in the Create Certificates - Operations Pane.

There are two search options, a basic search that includes only the user name, type, status and serial number fields, as well as an advanced search that includes all the search fields. The second option can only be performed by administrators with unlimited privileges.

Search Attributes

Basic Search Attributes

- **User name** - the exact string which is user name. By default this field is empty.
- **Type** - a drop-down list with the following options: Any, SIC, Gateway, Internal User or LDAP user, where the default is Any.
- **Status** - a drop-down list with the following options: Any, Pending, Valid, Revoked, Expired or Renewed (superseded), where the default is Any.
- **Serial Number** - the serial number of the requested certificate. By default this field is empty.

Advanced Search Attributes

This search includes all of the attributes described for the Basic Search, as well as the following:

- **Sub DN** - the string that represents the DN substring. By default this field is empty.
- **Valid From** - a text box with an option to open a calendar and select a date with the format dd-mmm-yyyy [hh:mm:ss] (for example 15-Jan-2003). By default this field is empty.
- **Valid To** - a text box with an option to open a calendar and select a date with the format dd-mmm-yyyy [hh:mm:ss] (for example 14-Jan-2003 15:39:26). By default this field is empty.
- **CRL Distribution Point** - a drop-down list with the following options: Any, No CRLDP (for certificates issued before the management upgrade - old CRL mode certificates) or any CRL number available, where the default is Any.

The Search Results

The results of the search are displayed in the Search Results pane. This pane consists of a table with a list of searched certificate attributes such as:
- (SN) Serial Number - the SN of the certificate.
- User Name (CN), a user name is considered a string that appears after the first "=" until the next comma ".
- DN.
- Status (where the statuses may be any of the following: Pending, Valid, Revoked, Expired, Renewed (superseded).
- The date from which the certificates are valid until the date that they are due to expire.

Search statistics will be displayed in the status bar after every search is performed.

**Viewing and Saving Certificate Details**

Click on the DN link in the Search Results pane in order to display certificate details.

- If the status is pending a window will be displayed which displays certificate information, including its registration key. In this case a log will be created and displayed in the SmartView Tracker.
- If the certificate was already created, a new window is displayed in which the certificate can be saved on a disk or opened directly, (assuming that this file extension is known to the operating system).

**Certificate Operations Using the ICA Management Tool**

Certificate operations (such as certificate creation) when done via the ICA Management Tool can only be used for user certificates.

⚠️ **Important** - SIC certificates and VPN certificates should not be modified using the ICA Management Tool, but via SmartDashboard.

Check the certificates on which you would like to perform the operations.

**Removing & Revoking Certificates and Sending Email Notifications**

1. Select Manage Certificates in the Menu pane. In the Manage Certificates - Operations pane:
2. Configure a search according to the required attributes, and click Search (see The ICA Management Tool GUI (on page 52)) The results are shown in the Search Results pane.
3. Select the requested certificates from the search results and click on one of the following three options:
   - Revoke Selected - this operation revokes the selected certificates. If a certificate is pending than this operation will remove it from the CA's database.
   - Remove Selected - this operation removes the selected certificates from the Database of the CA and from the CRL if it was found there. You can only remove expired or pending certificates.
   - Mail to Selected - this operation sends mail for all selected pending certificates that include the authorization codes to the selected users. Messages to users that do not have an email defined will be sent to a default address that can be defined in the CA Configuration window (select Menu pane > Configure the CA). For more information, see Notifying Users about Certificate Initialization (on page 52).

**Submitting a Certificate Request to the CA Using the ICA Management Tool**

There are three methods of submitting certificates:

- **Initiate** ("Initiating a Certificate" on page 57) - a registration key is created on the CA and used once by a user to create a certificate.
- **Generate** ("Generating a Certificate" on page 57) - a certificate file is created and associated with a password which must be entered whenever the certificate is accessed.
- **PKCS#10** ("Creating a PKCS#10 Certificate" on page 57) - when a PKCS#10 request for a certificate has been received, a certificate is created and delivered to the requester.
Initiating a Certificate

To initiate a certificate, proceed as follows:
1. In the Menu pane, select Create Certificates.
2. Select Initiate.
3. Enter a User Name or Full DN, or fill in the Form.
4. If you would like to enter expiration details for certificates or registration keys, click Advanced.
   - Certificate Expiration Date: open the calendar to select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss]. The default is two years from now.
   - Registration Key Expiration Date: open the calendar to select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss]. The default is two weeks from now.
5. Click Go. A registration key is created and displayed in the Results pane.
6. If desired, click Send mail to user to email the registration key. Note that the number of characters in the email is limited to 1900.
7. The certificate becomes usable upon supplying the proper registration key.

Generating a Certificate

To generate a certificate, proceed as follows:
1. In the Menu pane, select Create Certificates.
2. Select Generate.
3. Enter a User Name or Full DN, or fill in the Form.
4. If you would like to enter expiration details for certificates or registration keys, click Advanced.
   - Certificate Expiration Date: open the calendar to select a date or enter the date in the format dd-mm-yyyy [hh:mm:ss]. The default is two years from now.
   - Registration Key Expiration Date: open the calendar to select a date or enter the date in the format dd-mm-yyyy [hh:mm:ss]. The default is two weeks from now.
5. Enter a password.
6. Click Go.
7. Save the P12 file, and deliver it to the user.

Creating a PKCS#10 Certificate

To create a PKCS#10 certificate, proceed as follows:
1. In the Menu pane, select Create Certificates.
2. Select PKCS#10.
3. Either paste into the space the encrypted base-64 buffer text provided or click on Browse for a file to insert (IE only) to import the request file.
4. Click Create and save the resulting certificate.
5. Deliver the certificate to the requester.

Initializing Multiple Certificates Simultaneously

Bulk certificate initialization can be done as follows:
1. Create a file with the list of DNs that you want to initialize. There are two possible syntaxes for this file creation: LDAP or non-LDAP.
2. Browse for this file in the Advanced page of the Create Certificate page.
3. To send registration keys to the users, check the field Send registration keys via email.
4. To receive a file that lists the initialized DNs along with their registration keys, check the field Save results to file. This file can later be used by a script.
5. Click Initiate from file.

Using an LDAP Query

The format of the file initiated by the LDAP search is as follows:
- Each line after a blank line or the first line in the file represents one DN to be initialized.
If the line starts with "mail=" the string after contains the mail of that user. When no email is given the email address will be taken from the ICA’s "Management Tool Mail To Address" attribute.

If the line is not_after then the value at the next line is the Certificate Expiration Date in seconds from now.

If the line is otp_validity then the value at the next line is the Registration Key Expiration Date in seconds from now.

Example of Output of an LDAP Search

```
not_after  
86400  
otp_validity  
3600  
uid=user_1, ou=People, o=intranet, dc=company, dc=com  
mail=user_1@company.com  
<blank_line>
...  
uid=...  
```

For more information, see SmartDirectory (LDAP) and User Management (on page 115).

**Using a Simple Non-LDAP Query**

It is possible to create a simple (non-LDAP) query by configuring the DN + email in a file in the following format:

```
<email address> space <DN>
... blank line as a separator ...
<email address> space <DN>
```

**CRL Operations**

In the Menu pane, select Manage CRL and:

1. Either:
   - select Download and enter the number of the CRL that you would like to download, or
   - select Publish to immediately renew the current CRL after changes have been made to the CRL database (this operation is performed automatically at an interval set by the CRL Duration attribute).
   - select Recreate and enter the number of the CRL that you would like to recreate

2. Click Go.

**CA Cleanup**

On the Manage CRLs page, select Clean the CA’s Database and CRLs from expired certificates. This operation gets rid of all expired certificates. Before performing this operation, make sure that the time set on the Security Management server is accurate.
Configuring the CA

In the Menu pane, select **Configure the CA**. The Configure the CA - Operations pane displays all the configurable fields of the CA. There are three possible operations that can be performed:

- Select **Apply** to save and enter the CA configuration settings. If the values are valid, the configured settings will take effect immediately. All non-valid strings will be changed to the default value.
- Select **Cancel** to reset all values to the last configuration.
- Select **Restore Default** to revert the CA to its default configuration settings. Entering the string **Default** in one of the attributes will also reset it to the default after pressing **Configure**. Values that are valid will be changed as requested and others will change to default values.

**CA Data Types**

Edit the CA data by modifying the values displayed in the **Configure the CA - Operations Pane**. The CA data types can be any of the following:

- **Time** - displayed in the format: `<number> days <number> seconds`. For example: **CRL Duration**: 7 days 0 seconds.
  
  When changing the attribute, it can be entered as `<number> days <number> seconds` or just as a single number of seconds.

- **Integer** - a regular integer, for example: **SIC Key Size**: 1024.

- **Boolean** - the values can be true or false (not case sensitive). For example: **Enable renewal**: true.

- **String** - for example: **Management Tool DN prefix**: `cn=tests`.

The following attributes are listed in alphabetical order:

---

**Table 4-5 CA Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Comment</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Code Length</td>
<td>The number of characters of the authorization codes.</td>
<td>min-6 max-12</td>
<td>6</td>
</tr>
<tr>
<td>CRL Duration</td>
<td>The period of time for which the CRL is valid.</td>
<td>min-5 minutes max-1 year</td>
<td>1 week</td>
</tr>
<tr>
<td>Enable Renewal</td>
<td>For User certificates. This is a Boolean value setting which stipulates whether to enable renewal or not.</td>
<td>true or false</td>
<td>true</td>
</tr>
<tr>
<td>Grace Period Before Revocation</td>
<td>The amount of time the old certificate will remain in Renewed (superseded) state.</td>
<td><code>min-0 max-5 years</code></td>
<td>1 week</td>
</tr>
<tr>
<td>Grace Period Check Period</td>
<td>The amount of time between sequential checks of the Renewed (superseded) list in order to revoke those whose duration has passed.</td>
<td>min-10 minutes max-1 week</td>
<td>1 day</td>
</tr>
<tr>
<td>IKE Certificate Validity Period</td>
<td>The amount of time an IKE certificate will be valid.</td>
<td>min-10 minutes max-20 years</td>
<td>5 years</td>
</tr>
<tr>
<td>Attribute</td>
<td>Comment</td>
<td>Values</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>IKE Certificate Extended Key Usage</td>
<td>Certificate purposes for describing the type of the extended key usage for IKE certificates. Refer to RFC 2459.</td>
<td>means no KeyUsage</td>
<td></td>
</tr>
<tr>
<td>IKE Certificate Key usage</td>
<td>Certificate purposes for describing the certificate operations. Refer to RFC 2459.</td>
<td>Digital signature and Key encipherment</td>
<td></td>
</tr>
<tr>
<td>Management Tool DN prefix</td>
<td>Determines the DN prefix of a DN that will be created when entering a user name.</td>
<td>possible values</td>
<td>CN=</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN= UID=</td>
<td></td>
</tr>
<tr>
<td>Management Tool DN suffix</td>
<td>Determines the DN suffix of a DN that will be created when entering a user name.</td>
<td>ou=users</td>
<td></td>
</tr>
<tr>
<td>Management Tool Hide Mail Button</td>
<td>For security reasons the mail sending button after displaying a single certificate can be hidden.</td>
<td>true or false</td>
<td>false</td>
</tr>
<tr>
<td>Management Tool Mail Server</td>
<td>The SMTP server that will be used in order to send registration code mails. It has no default and must be configured in order for the mail sending option to work.</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Management Tool Registration Key Validity Period</td>
<td>The amount of time a registration code is valid when initiated using the Management Tool.</td>
<td>min-10 minutes max-2 months</td>
<td>2 weeks</td>
</tr>
<tr>
<td>Management Tool User Certificate Validity Period</td>
<td>The amount of time that a user certificate is valid when initiated using the Management Tool.</td>
<td>min-one week max-20 years</td>
<td>2 years</td>
</tr>
<tr>
<td>Management Tool Mail From Address</td>
<td>When sending mails this is the email address that will appear in the from field. A report of the mail delivery status will be sent to this address.</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Management Tool Mail Subject</td>
<td>The email subject field.</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Comment</td>
<td>Values</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------</td>
</tr>
</tbody>
</table>
| Management Tool Mail Text Format | The text that appears in the body of the message. 3 variables can be used in addition to the text: $REG_KEY (user's registration key); $EXPRIE (expiration time); $USER (user's DN). | Registration Key: $REG_KEY  
Expiration: $EXPRIE | -                           |
| Management Tool Mail To address | When the send mail option is used, the emails to users that have no email address defined will be sent to this address. | -                       | -                           |
| Max Certificates Per Distribution Point | The maximum capacity of a CRL in the new CRL mode. | min-3  
max-400               | 400                         |
| New CRL Mode                   | A Boolean value describing the CRL mode. | 0 for old CRL mode  
1 for new mode   | true                        |
| Number of certificates per search page | The number of certificates that will be displayed in each page of the search window. | min-1  
max-approx 700          | approx 700                  |
| Number of Digits for Serial Number | The number of digits of certificate serial numbers. | min-5  
max-10                 | 5                           |
| Revoke renewed certificates | This flag determines whether to revoke an old certificate after it has been renewed. The reason for not revoking this is to prevent the CRL from growing each time a certificate is renewed. If the certificate is not revoked the user may have two valid certificates. | true or false  
true              | false                       |
| SIC Key Size                   | The key size in bits of keys used in SIC. | possible values:  
1024  
2048  
4096               | 1024                        |
| SIC Certificate Key usage      | Certificate purposes for describing the certificate operations. Refer to RFC 2459. | Digital signature and Key encipherment | -                           |
| SIC Certificate Validity Period | The amount of time a SIC certificate will be valid. | min-10 minutes  
max-20 years   | 5 years                     |
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Comment</th>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Certificate Extended Key Usage</td>
<td>Certificate purposes for describing the type of the extended key usage for User certificates. Refer to RFC 2459.</td>
<td>means no KeyUsage</td>
<td></td>
</tr>
<tr>
<td>User Certificate Key Size</td>
<td>The key size in bits of the user's certificates.</td>
<td>Possible values are 1024 2048 4096</td>
<td>1024</td>
</tr>
<tr>
<td>User Certificate Key usage</td>
<td>Certificate purposes for describing the certificate operations. Refer to RFC 2459</td>
<td>Digital signature and Key encipherment</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 5

SmartView Tracker

In This Chapter

The Need for Tracking 63
The Check Point Solution for Tracking 64
Tracking Considerations 74
Tracking Configuration 75

The Need for Tracking

As a system administrator, you need an advanced tracking tool in order to:

- Ensure your products are operating properly, and to confirm that both basic operations such as access control and more advanced operations like IKE are all performing correctly.
- Troubleshoot system and security issues
- Gather information for legal reasons
- Generate reports to analyze your traffic patterns

You need different levels of tracking, depending on the data's importance. For example, while you may choose to track standard network patterns (e.g., your users' surfing patterns), this information is not urgent and you can inspect it at your convenience. However, if your network is being attacked, you must be alerted immediately.
The Check Point Solution for Tracking

Tracking Overview

Check Point products provide you with the ability to collect comprehensive information on your network activity in the form of logs. You can then audit these logs at any given time, analyze your traffic patterns and troubleshoot networking and security issues. The figure below illustrates the log collection and tracking process:

**Figure 5-8** Log Collection and Tracking Process

The SmartDashboard allows you to customize your tracking settings for each Rule Base, by specifying per-rule whether or not to track the events that match it.

If you decide to track the events that match a certain rule, you can choose from a variety of tracking options, based on the information's urgency. For example, you can choose a standard Log for allowed http connections; opt for an Account log when you wish to save byte data; or issue an Alert (in addition to the log) when a connection's destination is your gateway. For a list of the available tracking options, right-click the relevant rule's Track column.

The gateways on which this Policy is installed collect data as specified in the Policy, and forward the logs to the Security Management server (and/or to Log Servers, depending on their settings). The logs are organized in files according to the order in which they arrived to the Security Management server. All new logs are saved to the fw.log file, except for audit (management-related) logs, which are saved to the fw.adtlog file.

The Security Management server makes these logs available for inspection via SmartView Tracker - a comprehensive auditing solution, enabling central management of both active and old logs of all Check Point products. You can conveniently customize searches to address your specific tracking needs; integrate the logs with the Check Point SmartReporter; or export them to text files or to an external Oracle database.

The Security Management server also performs the operations specified in the Policy for events matching certain rules (e.g., issuing an alert, sending email, running a user-defined script etc.).

In addition to the above solutions, you can benefit from the tracking and auditing capabilities of the following Check Point SmartConsole:

- SmartView Monitor allows you to manage, view and test the status of various Check Point components throughout the system, as well as to generate reports on traffic on interfaces, specific Check Point products, and other Check Point system counters.
- SmartReporter allows you to save consolidated records (as opposed to "raw" logs) and conveniently focus on events of interest.

**Tracking Network Traffic**

The SmartView Tracker can be used to track all daily network traffic and activity logged by any Check Point and OPSEC Partners log-generating product. It can also be used to give an indication of certain problems. Network administrators can use the log information for:

- Detecting and monitoring security-related events.
For example, alerts, repeated rejected connections or failed authentication attempts, might point to possible intrusion attempts.

- Collection information about problematic issues.
  For example, a client has been authorized to establish a connection but the attempts to connect have failed. The SmartView Tracker might indicate that the Rule Base has been erroneously defined to block the client's connection attempts.

- Statistical purposes such as analyzing network traffic patterns.
  For example, how many HTTP services were used during peak activity as opposed to Telnet services.

**Log Suppression**

The SmartView Tracker is designed to efficiently present the logs that are generated from Check Point products. To avoid displaying log entries for a frequently repeating event, SmartView Tracker displays the first instance of the event and then counts subsequent instances which occur in the next two minutes.

For as long as the event continues to occur, every two minutes SmartView Tracker shows a Log Suppression Report which contains the details of the event as well as the number of times the event occurred.

**SmartView Tracker**

The figure below displays the main window of SmartView Tracker. Each entry in the Records pane is a record of an event that was logged according to a specific rule in the Rule Base. New records that are added to the fw.log file are automatically added to the Records pane as well.

To understand the figure, refer to the numbers in the figure and the following list.

1. The Network & Endpoint, Active and Management modes display different types of logs.
2. The Query Tree pane displays the Predefined and Custom queries.
3. The Query Properties pane displays the properties of the fields in the Records pane.
4. The Records pane displays the fields of each record in the log file.

**Figure 5-9** SmartView Tracker — Main Screen
The log fields displayed are a function of the following factors:

- The software blade that generated the log, such as Firewall, VPN or IPS.
- The type of operation performed, such as installation or opening a connection.

For example, when NAT is used, the address translation fields (with the ‘Xlate’ prefix, e.g., `XlateSrc`, `XlateDst` etc.) are displayed. When Firewall is used, IKE-related fields (e.g., `IKE Cookiel`, `IKE CookieR` etc.) are displayed.

**SmartView Tracker Actions**

The following table gives a description of the different types of actions recorded by SmartView Tracker.

<table>
<thead>
<tr>
<th>Action Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>The connection was allowed to proceed.</td>
</tr>
<tr>
<td>Reject</td>
<td>The connection was blocked.</td>
</tr>
<tr>
<td>Drop</td>
<td>The connection was dropped without notifying the source.</td>
</tr>
<tr>
<td>Detect</td>
<td>The connection was monitored without enforcing IPS protections.</td>
</tr>
<tr>
<td>Encrypt</td>
<td>The connection was encrypted.</td>
</tr>
<tr>
<td>Authcrypt</td>
<td>SecuRemote user logon.</td>
</tr>
<tr>
<td>Bypass</td>
<td>The connection passed transparently through InterSpect.</td>
</tr>
<tr>
<td>Flag</td>
<td>Flags the connection.</td>
</tr>
<tr>
<td>Login</td>
<td>A user logged into the system.</td>
</tr>
<tr>
<td>Reject</td>
<td>The connection was rejected.</td>
</tr>
<tr>
<td>VPN routing</td>
<td>The connection was routed through the gateway acting as a central hub.</td>
</tr>
<tr>
<td>Decrypt</td>
<td>The connection was decrypted.</td>
</tr>
<tr>
<td>Key Install</td>
<td>Encryption keys were created.</td>
</tr>
<tr>
<td>Authorize</td>
<td>Client Authentication logon.</td>
</tr>
<tr>
<td>Deauthorize</td>
<td>Client Authentication logoff.</td>
</tr>
<tr>
<td>Block</td>
<td>Connection blocked by Interspect.</td>
</tr>
<tr>
<td>Detect</td>
<td>Connection was detected by Interspect.</td>
</tr>
<tr>
<td>Inspect</td>
<td>Connection was subject to InterSpect configured protections.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>The IP source address of the connection was quarantined by InterSpect.</td>
</tr>
<tr>
<td>Replace Malicious code</td>
<td>Malicious code in the connection was replaced.</td>
</tr>
</tbody>
</table>
### Action Filter

<table>
<thead>
<tr>
<th>Action Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate / Disassociate</td>
<td>Identity Logging action.</td>
</tr>
</tbody>
</table>

### DLP Actions

Specific actions for DLP incidents include:

<table>
<thead>
<tr>
<th>DLP Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask User</td>
<td>DLP incident captured and put in Quarantine, user asked to decide what to do.</td>
</tr>
<tr>
<td>Do not Send</td>
<td>User decided to drop transmission that was captured by DLP.</td>
</tr>
<tr>
<td>Send</td>
<td>User decided to continue transmission after DLP notified that it may contain sensitive data.</td>
</tr>
<tr>
<td>Quarantine Expired</td>
<td>DLP captured data transmission cannot be sent because the user did not make a decision in time. Expired incidents may still be viewed, until they are deleted (routine cleanup process).</td>
</tr>
<tr>
<td>Prevent</td>
<td>DLP transmission was blocked.</td>
</tr>
<tr>
<td>Allow</td>
<td>DLP transmission was allowed; usually by exception to rule.</td>
</tr>
<tr>
<td>Inform User</td>
<td>DLP transmission was detected and allowed, and user notified.</td>
</tr>
<tr>
<td>Deleted Due To Quota</td>
<td>DLP incidents are deleted from gateway for disk space.</td>
</tr>
<tr>
<td>Incident Reviewed</td>
<td>DLP incident data has been reviewed.</td>
</tr>
</tbody>
</table>

### SmartView Tracker Other Columns

Other than actions, other columns may be presented, depending on enabled Software Blade and how the incident was matched.

This list is not comprehensive.

### IPS Columns

The **Protection Type** column is relevant to IPS protection incidents. You can filter for any of these types:

- Application Control
- Engine Settings
- Geo Protection
- Protocol Anomaly
- Signature

Other columns specific to the IPS Software Blade:

- Protected Server
- Source Reputation
- Destination Reputation
- Client Type
- Server Type
DLP General Columns

DLP incidents may show any of these columns and are available to all administrators.

<table>
<thead>
<tr>
<th>DLP Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident UID</td>
<td>Unique ID of the incident.</td>
</tr>
<tr>
<td>DLP Action Reason</td>
<td>Reason for the action. Possible values: Rulebase, Internal Error, Prior User Decision</td>
</tr>
<tr>
<td>Related Incident</td>
<td>Internal incident ID related to the current log.</td>
</tr>
<tr>
<td>DLP Transport</td>
<td>Protocol of the traffic of the incident: HTTP, FTP, SMTP.</td>
</tr>
</tbody>
</table>

Using the Incident UID as a key between multiple logs:

Each DLP incident has a unique ID included in the log and sent to the user as part of an email notification. User actions (Send, Do not Send) are assigned the same Incident UID that was assigned to the original DLP incident log.

If a user sends an email with a DLP violation and then decides to discard it, two logs are generated. The first log is a DLP incident log with Ask User action and is assigned an Incident UID. On the user action, the second log is generated with the same UID, with the Do not Send action.

Each matched data type generates its own log. The gateway makes sure that all the data type logs of one incident indicate the same unique Incident UID and rule action (Prevent, Ask, Inform, or Detect), even if data types were matched on different rules. The common action for an incident is the most restrictive.

For example, assume a transmission matches two data types. Each data type is used in a different rule. The action of one rule is Prevent. The action of another rule is Detect. The two logs that are generated will indicate Prevent as the action. (The action implemented will be Prevent.) The log of the Detect rule will show Rule Base (Action set by different rule) in the DLP Action Reason column.

DLP Restricted Columns

These columns are restricted to administrators with permissions.

<table>
<thead>
<tr>
<th>Restricted Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Rule Name</td>
<td>Name of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Rule UID</td>
<td>Internal rule ID of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>Data Type UID</td>
<td>Internal ID of the data type on which the incident was matched.</td>
</tr>
<tr>
<td>Data Type Name</td>
<td>Name of the matched data type.</td>
</tr>
<tr>
<td>User Action Comment</td>
<td>Comment given by user when releasing the incident from the Portal.</td>
</tr>
<tr>
<td>DLP Recipients</td>
<td>For SMTP traffic, list of recipients of captured email.</td>
</tr>
<tr>
<td>Scanned Data Fragment</td>
<td>Captured data itself: email and attachment of SMTP, file of FTP, or HTTP traffic.</td>
</tr>
<tr>
<td>Message to User</td>
<td>Message sent, as configured by administrator, for the rule on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Categories</td>
<td>Category of data type on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Words List</td>
<td>If the data type on which the incident was matched included a word list (keywords, dictionary, and so on), the list of matched words.</td>
</tr>
</tbody>
</table>
### Restricted Filters

<table>
<thead>
<tr>
<th>Description</th>
<th>Mail Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>For SMTP traffic, the subject of captured email.</td>
<td></td>
</tr>
</tbody>
</table>

### Identity Logging Columns

Incidents for Identity Logging show information about the AD name and IP address associations.

<table>
<thead>
<tr>
<th>Identity Logging Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Machine Name</td>
<td>Resolved AD name of a machine associated with destination IP of a logged traffic.</td>
</tr>
<tr>
<td>Destination User Name</td>
<td>Resolved AD name of a user associated with destination IP of a logged traffic.</td>
</tr>
<tr>
<td>Source Machine Name</td>
<td>Resolved AD name of a machine associated with source IP of a logged traffic.</td>
</tr>
<tr>
<td>Source User Name</td>
<td>Resolved AD name of a user associated with source IP of a logged traffic.</td>
</tr>
</tbody>
</table>

### IPS-1 Columns

These columns are relevant for IPS-1 appliances.

<table>
<thead>
<tr>
<th>IPS-1 Product Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPC Service Number</td>
<td>Protocol detail.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Internal ID of the VLAN.</td>
</tr>
<tr>
<td>MAC Destination Address</td>
<td>MAC address associated with destination or source machine.</td>
</tr>
<tr>
<td>MAC Source Address</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Used in protocol context and is name or identifier of the command used in the traffic of the attack.</td>
</tr>
<tr>
<td>Destination DHCP Hostname</td>
<td>Name of the host associated with source or destination of the logged traffic according to the relevant resolving service. Not all those fields are filled in the same time.</td>
</tr>
<tr>
<td>Destination DNS Hostname</td>
<td></td>
</tr>
<tr>
<td>NetBIOS Destination Hostname</td>
<td></td>
</tr>
<tr>
<td>NetBIOS Source Hostname</td>
<td></td>
</tr>
<tr>
<td>Source DHCP Hostname</td>
<td></td>
</tr>
<tr>
<td>Source DNS Hostname</td>
<td></td>
</tr>
<tr>
<td>Source OS</td>
<td>OS type of source or destination machine.</td>
</tr>
<tr>
<td>Destination OS</td>
<td></td>
</tr>
<tr>
<td>Email Address</td>
<td>Email address fetched from attack traffic.</td>
</tr>
<tr>
<td>Email Subject</td>
<td>Subject of the email caught in attack traffic.</td>
</tr>
<tr>
<td>Hostname</td>
<td>If in attack traffic we find host name that is unrelated to the either source or destination, it is given here.</td>
</tr>
<tr>
<td>HTTP Referer</td>
<td>HTTP protocol elements.</td>
</tr>
<tr>
<td>HTTP Modifier</td>
<td></td>
</tr>
<tr>
<td>Cookie</td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td></td>
</tr>
<tr>
<td>Payload</td>
<td></td>
</tr>
<tr>
<td>IPS-1 Product Column</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Attack Assessment</td>
<td>Possible values: Failed, Successful, Unknown.</td>
</tr>
<tr>
<td>Sensor Mode</td>
<td>Possible values: Invalid, Passive, Inline - Fail-open, Inline - Fail-closed, Inline - Monitor only.</td>
</tr>
<tr>
<td>Activated Quarantine</td>
<td>Whether attack caused quarantine.</td>
</tr>
</tbody>
</table>

**SmartView Tracker Modes**

SmartView Tracker consists of three different modes:

- **Log**, the default mode, displays all logs in the current `fw.log` file. These include entries for security-related events logged by different Check Point software blades, as well as Check Point's OPSEC partners. New logs that are added to the `fw.log` file are added to the bottom of the Records pane.

- **Active** allows you to focus on connections that are currently open through the Security Gateways that are logging to the active Log file.

- **Audit** allows you to focus on management-related records, such as records of changes made to objects in the Rule Base and general SmartDashboard usage. This mode displays audit-specific data, such as the record's *Administrator*, *Application* or *Operation* details, which is read from the `fw.adtlog` file.

You can toggle between modes by clicking the desired tab.

**Filtering**

SmartView Tracker’s filtering mechanism allows you to conveniently focus on log data of interest and hide other data, by defining the appropriate criteria per-log field. Once you have applied the filtering criteria, only entries matching the selected criteria are displayed.

The filtering options available are a function of the log field in question. For example, while the Date field is filtered to show data that is after, before or in the range of the specified date, the Source, Destination and Origin fields are filtered to match (or differ from) the specified machines.

It is very useful to filter the Product field and focus on a specific Check Point product. SmartView Tracker features these filters as predefined queries.

**Queries**

SmartView Tracker gives you control over the Log file information displayed. You can either display all records in the Log file, or filter the display to focus on a limited set of records matching one or more conditions you are interested in. This filtering is achieved by running a query.

A query consists of the following components:

- Condition(s) applied to one or more log fields (record columns) — for example, to investigate all HTTP requests arriving from a specific source, you can run a query specifying HTTP as the Service column's filter and the machine in question as the Source column's filter.

- A selection of the columns you wish to show — for example, when investigating HTTP requests it is relevant to show the URL log field.

Each of the SmartDashboard's three modes (Log, Active and Audit) has its own Query Tree, consisting of the following folders:

- **Predefined**: contains the default queries that cannot be directly modified or saved.
The predefined queries available depend on the mode you are in. The default query of all three modes is **All Records**. In addition, the **Log** mode includes predefined per product or feature.

- **Custom**: allows you to customize your own Query based on a predefined one, to better address your needs. Customized queries are the main querying tool, allowing you to pinpoint the data you are interested in. An existing query that is copied or saved under a new name is automatically added to the **Custom** folder.

The attributes of the selected query are displayed in the **Query Properties** pane.

**Matching Rule**

SmartView Tracker records the Firewall Rule Base rule to which a connection was matched. The matching rule is recorded in four columns in SmartView Tracker, as depicted in the figure below:

![Figure 5-10 Recording the Matching Rule](image)

- The **Rule** column, which records the number of the rule in the Rule Base at the time the log entry was recorded. Like other properties in SmartView Tracker, logs can be sorted and queried by rule number.

- The **Current Rule Number** column, which is a dynamic field that reflects the current placement of the rule in the Rule Base and displays the current policy package name. As the Rule Base is typically subject to change, this column makes it possible to locate the rules that have changed their relative positions in the Rule Base since the log was recorded, and to create filters for log entries that match the rule, not just the rule number. By way of example, note the log entry in the figure. When this log was first recorded, it recorded the matching rule as Rule 1. Since then the rule's position in the Rule Base has changed, and so the **Current Rule Number** column reports its present position as 2 [Standard], where [Standard] is the name of the policy package in which this rule resides.

- The **Rule Name** column, which records the short textual description of the rule in the **Name** column of the Rule Base, when in use.

- The **Rule UID** column, which records the unique identifying number (UID) that is generated for each rule at the time that it is created. This number serves an internal tracking function, and as such the column is hidden by default. To display this column, click on **View > Query Properties** and enable the **Rule UID** property.

**Filtering Log Entries by Matching Rule**

In order to filter log entries based on a matching rule, right-click on a log entry and choose either **Follow Rule** or **Follow Rule Number**.

- **Follow Rule** generates a filtered view of all logs that matched this rule, and is based on the UID number of the rule.

- **Follow Rule Number** generates a filtered view of all log files that match the number recorded in the **Rule** column of the selected log.

These two operations are essentially short-cuts to creating a filter. You can achieve the same results by right-clicking anywhere in a given column and selecting **Edit Filter**, and then entering the filtering criteria you want to apply.
The Rule and Current Rule Number filters, which provide the same functionality as the Follow Rule and Follow Rule Number commands, can also create filtered views based on multiple matching rules. The figure below shows the Current Rule Number Filter.

**Figure 5-11** Current Rule Number Filter

For configuration information, see Configuring the Current Rule Number Filter (on page 77).

**Viewing the Matching Rule in Context**

From SmartView Tracker, you can launch SmartDashboard to examine the rule within the context of the Firewall Rule Base. By right-clicking on the relevant log and selecting View rule in SmartDashboard, SmartDashboard will open with the rule highlighted in white.

If you are using version control, SmartDashboard opens with the revision that was saved when this record was created. If no revision is available, SmartDashboard uses the unique identifying number to display the relevant rule. If neither version control nor a UID number are available, the View rule in SmartDashboard option is not available.

**Viewing the Logs of a Rule from SmartDashboard**

From the firewall Rule Base in SmartDashboard, there are two methods by which you can launch SmartView Tracker to view all of the log entries that matched on a particular rule. By right-clicking on the rule, you can choose to either:

- View rule logs in SmartView Tracker, which opens SmartView Tracker to a filtered view of all logs that matched on the rule.
- Copy Rule ID, which copies the unique identifying number of the rule to the clipboard, allowing the user to paste the value into the Rule UID Filter in SmartView Tracker.

For detailed instructions, see Viewing the Logs of a Rule from the Rule Base (on page 78).

**Log File Maintenance via Log Switch**

The active Log file's size is kept below the 2 GB default limit by closing the current file when it approaches this limit and starting a new file. This operation, known as a log switch, is performed either automatically, when the Log file reaches the specified size or according to a log switch schedule; or manually, from SmartView Tracker.

The file that is closed is written to the disk and named according to the current date and time. The new Log file automatically receives the default Log file name ($FWDIR/log/fw.log for log mode and $FWDIR/log/fw.adtlog for audit mode).

**Disk Space Management via Cyclic Logging**

When there is a lack of sufficient free disk space, the system stops generating logs. To ensure the logging process continues even when there is not enough disk space, you can set a process known as Cyclic Logging. This process automatically starts deleting old log files when the specified free disk space limit is reached, so that the Security Gateway can continue logging new information. The Cyclic Logging process is controlled by:

- Modifying the amount of required free disk space.
• Setting the Security Gateway to refrain from deleting logs from a specific number of days back.

Log Export Capabilities

While SmartView Tracker is the standard log tracking solution, you may also wish to use your logs in other ways that are specific to your organization. For that purpose, Check Point products provide you with the option to export log files to the appropriate destination.

A log file can be exported in two different ways:

• As a simple text file

• In a database format, exported to an external Oracle database

SmartView Tracker supports a basic export operation, in which the display is copied as-is into a text file. More advanced export operations (for example, exporting the whole log file or exporting logs online) are performed using the command line (using the fwm logexport, log_export and fw log commands).

With the Export option (File > Export) you can create a comma delimited ASCII file that can be used as input for other applications.

Local Logging

By default, Security Gateways forward their log records online to the Security Management server. Alternatively, to improve the gateway’s performance, you can free it from constantly sending logs by saving the information to local log files. These files can either be automatically forwarded to the Security Management server or Log Server, according to a specified schedule; or manually imported through SmartView Tracker, using the Remote File Management operation.

Logging Behavior During Downtime

During downtime, when the gateway cannot forward its logs, they are written to a local file. To view these local files, you must manually import them using the Remote File Management operation.

Logging Using Log Servers

To reduce the load on the Security Management server, administrators can install Log Servers and then configure the gateways to forward their logs to these Log Servers. In this case, the logs are viewed by logging with SmartView Tracker into the Log Server machine (instead of the Security Management server machine).

A Log Server behaves just like a Security Management server for all log management purposes: it executes the operation specified in the Policy for events matching certain rules (e.g., issuing an alert or an email); performs an Automatic Log Switch when fw.log reaches 2GB, allows you to export files, etc.

Setting Up Security Management Server for Log Server

Logs are not automatically forwarded to new log servers. You must manually setup each relevant gateway to send its logs to the new log server. The same plug-ins should be installed on all Security Management servers and log servers involved in order for the install policy procedure to be successful.

To instruct a Security Management server to send logs to a Log server:

1. In SmartDashboard, double-click the gateway object to display its Check Point Gateway window.
2. Select Logs and Masters > Additional Logging. Select Forward log files to Log Server.
   
   The Security Management server drop-down list is enabled.
3. Select the new log server from the Security Managements drop-down list and click OK.
4. Select Policy > Install, and then select the gateways and log servers on which the Policy should be installed.
Check Point Advisory

Check Point Advisory are detailed descriptions and step-by-step instructions on how to activate and configure relevant defenses provided by Check Point and IPS Updates.

The ability to view a Check Point Advisory in SmartView Tracker provides information about the IPS protection that is directly related to the selected IPS log. This information can help you analyze your configuration choices and better understand why the specific SmartView Tracker log appeared.

In addition, Check Point Advisory supplies all of your IPS configuration choices so that you can learn why the specific log appeared. To view Check Point Advisory for a specific IPS log, right-click the log and select Go to Advisory.

For more detailed information about the IPS log and associated protection, scroll down to the bottom of the Check Point Advisory window and select Read the Full ADVISORY and SOLUTION.

The Check Point Advisory feature will not appear for logs that do not contain an Attack Name and/or Attack Information.

Advanced Tracking Operations

Blocking Intruders

The Active mode of SmartView Tracker allows you to shut out intruders by selecting the connection you've identified as intrusive and blocking one of the following. Block Intruder uses SAM to perform the block action.

- The connection - block the selected connection or any other connection with the same service, source or destination.
- The source of the connection - block access to and from this source. Block all connections that are headed to or coming from the machine specified in the Source field.
- The destination of the connection - block access to and from this destination. Block all connections that are headed to or coming from the machine specified in the Destination field.
- Specify a time frame during which this connection is to be blocked.

Running Custom Commands

SmartView Tracker allows you to conveniently run commands from the SmartConsole, instead of working in the command line. The commands available by default are ping and whois. These commands, along with the ones you add manually, are available through the menu displayed by right-clicking a relevant cell in the Records pane.

Viewing Packet Capture

Certain Check Point products include the ability to capture network traffic. After this feature is activated, a packet capture file is sent with a log to the log server. The packet capture can be retrieved at a later time to allow the administrator greater insight into the exact traffic which generated the alert.

The packet capture file can be accessed from the log entry in SmartView Tracker. The file can be saved as a file to a file location, or can be opened in the internal viewer included in the SmartConsole or any packet capture viewer installed on the SmartConsole client.

Tracking Considerations

Choosing which Rules to Track

The extent to which you can benefit from the events log depends on how well they represent the traffic patterns you are interested in. Therefore, you must ensure your Security Policy is indeed tracking all events you may later wish to study. On the other hand, you should keep in mind that tracking multiple events results in an inflated log file, which requires more disk space and management operations.
To balance these conflicting needs, and determine which of your Policy's rules should be tracked, consider how useful this information is to you. For example, consider whether this information:

- Improves your network's security
- Enhances your understanding of your users' behavior
- Is the kind of data you wish to see in reports
- May be useful for future purposes

### Choosing the Appropriate Tracking Option

For each rule you track, specify one of the following tracking options:

- **Log** - saving the event's details to your log file, for future reference. This option is useful for obtaining general information on your network's traffic.
- **Account** - required for including byte information in the record you save.
- **Alert** - allowing you to both log the event and set the Security Management server to execute a relevant command: display a popup window, send an email alert or an SNMP trap alert, or run a user-defined script.

### Forwarding Online or Forwarding on Schedule

By default, Security Gateways forward their log records online, one by one, to the selected destination (the Security Management server or a Log Server). In this case, SmartView Tracker allows you to see new records as they are forwarded to the machine you logged into.

To improve the gateway's performance, you can free it from constantly forwarding logs by configuring a Local Logging system in which the records are saved to a local log file. If you set a log forwarding schedule, you can open this file (instead of the active file) in SmartView Tracker. Otherwise, you can manually import this file from the gateway, using the **Remote File Management** operation.

### Modifying the Log Forwarding Process

Log files can be forwarded without deleting them from the Security Management server, Security Gateway, or Log server that sends them. This is particularly useful in a Provider-1 environment.

In a Provider-1 environment logs are commonly saved on the customer's Log server, to which the customer connects using SmartView Tracker. However, for analysis and back-up purposes, these logs are soon forwarded to dedicated servers run by the customer's ISP, to which the customer has no access. This enhancement to the scheduled log forwarding process makes the logs available to both the customer and customer's ISP.

By default, this feature is disabled. To enable the feature, use GuiDBEdit to set the **forward_log_without_delete** property to **TRUE**.

**Note** - If cyclical logging has been enabled, the log files maintained on the sender after forwarding will eventually be overwritten.

### Tracking Configuration

#### Basic Tracking Configuration

To track connections in your network:

1. For each of the Security Policy rules you wish to track, right-click in the **Track** column and choose **Log** from the menu. All events matching these rules are logged.
2. Launch SmartView Tracker through the SmartDashboard's **Window** menu.
The Log mode is displayed, showing the records of all events you have logged.

**SmartView Tracker View Options**

The display of SmartView Tracker can be modified to better suit your auditing needs. The following table lists the operations you can perform to adjust the view.

*Table 5-6  SmartView Tracker View Options*

<table>
<thead>
<tr>
<th>Operation</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toggling the display of the Query Tree and Query Properties panes</td>
<td>Choose View &gt; Query Tree or Query Properties (respectively).</td>
</tr>
</tbody>
</table>
| Resizing columns                               | Choose one of the following:  
  - In the Query Properties pane — enter the appropriate number of characters in the Width column, or  
  - In the Records pane — drag the column's right border while clicking on the left mouse button. Release when the column has reached its desired width. |
| Sorting columns                                | Choose one of the following:  
  - In the Query Properties pane — drag the column up or down to the desired position, or  
  - In the Records pane — drag the header of the column left or right to the desired position. |
| Collapsing/expanding the Query Tree            | Selecting (+) or (-), respectively. |
| Display a record's details window              | Double-click the record in question in the Records pane. |

**Query Pane**

The Query Tree pane is the area where the Log Files appear. The SmartView Tracker has a new and improved interface enabling you to open multiple windows.

You can open more than one Log File simultaneously. You can also open more than one window of the same Log File. This may be helpful if you want to get different images of the same Log File. For example, you can open two windows of the same file and use different filtering criteria on each window. You can view both windows simultaneously and compare the different images. You can also resize each window so as to fit in as many windows as possible in the Query pane. The Query pane is divided into two sections:

- **Query Properties pane** shows all the attributes of the fields contained in the Records pane.
- **Records pane** displays the fields of each record in the Log File.

**Resolving IP Addresses**

Since the IP address resolution process consumes time and resources, SmartView Tracker allows you to choose whether or not to display source and destination host names in the Log file.

Click the Resolve IP toolbar button to toggle between:

- Displaying the name of the host and the domain.
- Displaying the addresses in conventional IP dot notation.
Resolving Services

With the Resolving Services option you can control the display of the source and destination port in the Log File. Each port number is mapped to the type of service it uses.

This option toggles between:

- Displaying the destination port number.
- Displaying the type of service the port uses.

Note - If you clicked the Resolving Services button to display the type of service the port uses, and the port number appears, it means that a service has not been previously defined for this port. A port number can be mapped to a service either in the Objects database using the Object Manager or in the Services Configuration file. In SecurePlatform, the Services Configuration file name is called /etc/services

Showing Null Matches

This option controls the display of Null Matches, that is, log entries that are neither included nor excluded by the current filtering criteria.

For example, if you choose to display only log entries whose Action is either Reject or Drop, control logs are null matches because Action is not relevant to a control log. They are neither included nor excluded. If the Show Null Matches toolbar button is clicked, the null matches are displayed.

Configuring a Filter

To filter a log field and focus on data of interest:

1. Choose one of the following:
   - Display the Query Properties pane (by selecting View > Query Properties) and right-click the desired log field in the Filter column, or
   - In the Records pane, right-click the log field (e.g., the column) you wish to filter.
     The right-click menu is displayed.

2. Choose Edit Filter from the displayed menu.
   Each field displays a type-specific Filter window. Configure the window as desired and the log data will be displayed according to the filtering criteria used.

3. Click OK to apply the filter settings.

Note - Filtering criteria takes effect only if the Apply Filter toolbar button is activated.

Configuring the Current Rule Number Filter

To launch the Current Rule Number Filter:

1. Right-click anywhere in the column Curr. Rule No. and select Edit Filter.
2. Select the appropriate policy package from the drop-down list.
3. Select the current rule number(s) of the logs you want to display and click OK.
Follow Source, Destination, User Data, Rule and Rule Number

With the Follow commands you can create a filter that matches a specific query to a specific Source, Destination or User.

Right-click the record with the value of interest in the Records pane and select one of the following Follow commands:

- **Follow Source** enables a search for a log record according to a specific source.
- **Follow Destination** enables a search for a log record according to a specific destination.
- **Follow User** enables a search for a log record according to a specific user.
- **Follow Rule Number** enables a search for a log record according to the rule name.
- **Follow Rule** enables a search for a log record according to the rule number.

**Note** - A new window opens, displaying the relevant column (Source, Destination or User) first.

Viewing the Logs of a Rule from the Rule Base

From the Rule Base in SmartDashboard, it is possible to generate a filtered view of logs that match a specific rule. There are two ways of achieving this:

- **View rule logs in SmartView Tracker**
  a) Right-click on a rule in the No. column in SmartDashboard and select View rule logs in SmartView Tracker.
  
  SmartView Tracker opens with a filter applied to the Curr. Rule No. column to display only those logs that match on the selected rule.

- **Copy rule ID**
  a) Right-click on the rule in the No. column in SmartDashboard and select Copy rule ID.
  
  b) In SmartView Tracker, click View > Query Properties and enable the Rule UID column.
  
  c) Right-click on the Rule UID column heading and choose Edit Filter.
  
  d) Paste the UID in the Value field and click OK.
  
  A filter is applied to the Curr. Rule No. column to display only those logs that matched on the Rule UID.

Configuring Queries

New queries are created by customizing existing queries and saving them under new names. Proceed as follows:

1. Select an existing query in the Query Tree (either a predefined query or a custom query) and choose Query > Copy from the menu.
   
   A copy of the query, named New, is added to the Custom folder.
2. Rename the new query.
3. In the Query Properties pane, modify the query as desired by specifying the following for each relevant log field (column):
   - Whether to Show the information available for that column.
   - The Width of the column displaying the information.
   - The Filter (conditions) applied to the column.
4. Double-click the query in order to run it.

**Opening An Existing Query**

You can open an existing query in an active window by:

- Using the **Query** menu:
  In the **Query Tree pane**, select the query you would like to open. Select **Query > Open**. The desired query appears in the **Records** pane.

- Right-clicking an existing query.
  Right-click the query you would like to open. Select **Open**. The desired query appears in the **Records** pane.

- Double-clicking an existing query.
  Double-click the query you would like to open. The desired query appears in the **Records** pane.

**Creating A Customized Entry**

**Predefined** queries contained in the **Predefined** folder cannot be modified but they can be saved under a different name.

**To save a predefined query under a different name:**

1. Open a **predefined** query.
2. Modify the query as desired.
3. From the **Query** menu, select **Save As**.
4. Type the desired query name.
5. Click **OK**. The modified view is placed in the **Custom** folder.

**Saving a Query Under a New Name**

You can modify a query and save it under a new name.

**To modify a predefined Query and save it under a new name:**

1. Modify the predefined query as desired.
2. Choose **Save As** from the **Query** menu, and specify a file name for the modified query.
3. Click **OK**. The modified query is placed in the **Custom** folder.

**To save the changes made to a custom Query**

1. Modify the query as desired.
2. Choose **Save** from the **Query** menu.

**Renaming a Customized Query**

1. Select the query you want to rename.
   - From the **Query** menu, select **Rename**, or
   - Right-click the desired query and select **Rename** from the displayed menu. The newly-duplicated query is placed in the **Custom** folder.
2. Enter the desired query name and click **Enter**.

**Deleting a Customized Query**

Select the query you want to delete:

- From the **Query** menu, select **Delete**, or
- Right-click the desired query and select **Delete** from the displayed menu.
Note - You cannot delete an open or predefined query.

Hiding and Showing the Query Tree Pane
You can choose to hide or display the Query Tree pane. To toggle the display of the Query Tree pane click Query Tree from the View menu.

Working with the Query Properties Pane
The Query Properties pane shows the attributes for the corresponding columns in the Records pane. These attributes include whether the columns are displayed or hidden, the width of the column and the filtering arguments you used to display specific entries.

The Query Properties pane contains four columns.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>The name of the column</td>
</tr>
<tr>
<td>Show</td>
<td>Select to display the corresponding column in the Records pane. Deselect to conceal the corresponding column</td>
</tr>
<tr>
<td>Width</td>
<td>The specified width of the corresponding column in the Records pane in pixels</td>
</tr>
<tr>
<td>Filter</td>
<td>The items contained in this column represent the filtering criteria used to display specific log data</td>
</tr>
</tbody>
</table>

Modifying a Column's Properties

Showing/Hiding a Column

- Using the Query Properties pane
  In the Query Properties pane, select the column's check box in the Show column to display the column or clear the check box to hide it. The corresponding column in the Records pane is displayed/hidden respectively.

- Using the Records pane
  In the Records pane, right-click the column heading. Select Hide from the displayed menu. The column is hidden and at the same time, the check box in the Show column in the Query Properties pane is automatically cleared.

Changing a Column's Width
If you change the width of a column in one pane, it is automatically changed in the other. You can change the width of a column either in the:

- Query Properties pane
  Double-click the Width field that you would like to edit in the Width column. The Width field becomes an editable field in which you can specify a new width (in pixels). Edit the width value and click Enter. The corresponding column in the Records pane is widened/narrowed accordingly.

- Records pane
  Place the cursor on the column's right border in the header. The cursor changes to the column resize cursor. Click on the left mouse button without releasing it. Move the column border to the desired position while keeping the left mouse button down. Release the left mouse button. The value in the column's corresponding Width field in the Query Properties pane is automatically modified accordingly.
Rearranging a Column’s Position

You can rearrange a column's position in the Query Properties or the Records pane. If you change the position in one pane, it is automatically changed in the other.

- In the Queries Properties pane, drag the column up or down to the desired position.
- In the Records pane, drag the header of the column left or right to the desired position.

Copying Log Record Data

You can copy a whole log record or only one of its cells to the clipboard:

- Right-click the desired record.
- Select Copy Cell from the displayed menu to copy only the cell on which the cursor is standing or select Copy Line to copy the entire record.

Viewing a Record's Details

The Record Details window is displayed by double-clicking the desired record in the Records pane. This window allows you to conveniently view the record's values for all fields included in your query. Fields that have been defined as hidden for that record are not displayed. The fields appear in the same order as they appear in the Records pane, and all field values appear in their entirety, as can be seen in the tool tip.

This window allows you to perform the following operations:

- Display the details of the former or subsequent record by clicking the Previous or Next button respectively. (These buttons correspond to the keyboard arrows.)
- Copy the record details to the clipboard by clicking Copy.
- Change the colors of the Record Details window by clicking Switch Colors.
- End operations that take a long time by clicking Abort (this button is enabled only when the server is running).

Note - The Abort option only becomes active when a certain action is being executed, for example, when the Log File is being updated or when a search is taking place.

Viewing a Rule

You can view the rule that created the log.

**To view a rule:**

1. Open SmartDashboard.
   a) Click the Database Revision Control toolbar button.
   b) Click inside the Create new version upon Install Policy operation check box.
   c) Click Close.
   d) Click Install Policy.
2. Go to SmartView Tracker.
3. Right-click on the desired record.
4. Select View Rule in SmartDashboard. The SmartDashboard is opened and the rule appears.
Note - This process only works for logs that have a rule number and were created after the Create a new version upon Install Policy operation is selected. In addition, this option is only available on a Management Station. It is not available on CLM (Customer Log Module).

Find by Interface
To find by interface, add the specific Interface. You can find according to direction forward and back.

Maintenance
The following maintenance operations apply to all logging systems, whether the logs are forwarded to the Security Management server (the default setting), sent to Log Servers or saved locally.

Managing the Log Switch Settings
A log switch can be performed in one of the following ways:

- Automatically, when the log file’s size is 2 GB.
  You can modify this default size limit, as well as define a log switch schedule, through the SmartDashboard, by editing the properties of the object collecting the logs (the Security Management server, Log Server or the Security Gateway).

- Manually, from SmartView Tracker.

Modifying the Automatic Log Switch Settings
1. In the SmartDashboard, double-click the gateway in question. The gateway’s properties window is displayed.
2. In the Log switch section of the Logs and Masters page, specifies when to perform the log switch:
   - To specify the file size that should trigger a log switch, check Log switch when file size is x MBytes and specify the appropriate size.
   - To setup a log switch schedule, check Schedule log switch to and choose the appropriate time object from the drop-down list.
   - If you specify both options, the log switch is performed when the first criterion is met.
3. Click OK.

Manual Log Switch
1. In SmartView Tracker, choose File > Switch Active File from the menu. The Switch active Log File window is displayed.
2. By default, the current log file is named based on the current date and time.
   To specify a different name, uncheck Default and enter the appropriate name under Log File Name.

Managing the Cyclic Logging Settings
To configure the Cyclic Logging process:
1. In the SmartDashboard, double-click the gateway in question. The gateway’s properties window is displayed.
2. In the Disk Space Management section of the Logs and Masters page, specify the following:
   - Whether to Measure free disk space in MBytes or Percent.
   - Check Required Free Disk Space and enter the appropriate value.
   - To refrain from deleting the most recent log files among your old log files, check Do not delete log files from the last and specify the appropriate number of Days.
Purging a Log File

To delete all records in the active \texttt{fw.log} log file, display the Log or Audit mode and choose Purge Active File from the File menu.

Local Logging

To save logs to a local file (instead of forwarding them to the Security Management server or to a Log Server):

1. In the SmartDashboard, double-click the gateway in question to display its properties window.
2. In the Log Servers page (under the Logs and Masters branch), check Define Log Servers and then check Save logs locally, on this machine (<machine hostname>).
3. You can either set a schedule for forwarding the local file to the appropriate machine (the Security Management server or a Log Server), or manually import these files using SmartView Tracker.

To specify a log file forwarding schedule:
- Display the Additional Logging Configuration page (under the Logs and Masters branch).
- In the Log forwarding settings section, set the following:
  - Check Forward log files to Security Management server and choose the Log Server from the drop-down list.
  - Set a Log forwarding schedule by choosing the appropriate time object from the drop-down list.

To view the local file using SmartView Tracker:

1. Select Tools > Remote Files Management. The Remote Files Management window is displayed, listing all Security Gateways from which you can fetch Log files.
2. Select the desired Security Gateway and click Get File List. The Files on <Gateway Name> window is displayed, listing all Log files found on the selected Security Gateway.
3. Select one or more files to be fetched.
   
   Note - You cannot fetch an active Log File. If you want to fetch the current file, you must first perform a log switch.

4. Click Fetch Files. The Files Fetch Progress window is displayed, showing the progress of the file transfer operation.

Working with Log Servers

To reduce the Security Management server's load via Log Servers:

1. Install the Log Server software on the machine you wish to dedicate to logging purposes.

   Note - For proper Log Server operations, the Plug-ins that are installed on the Security Management server should also be installed on the Log Server.

2. Launch the SmartDashboard and add the Log Server you have installed as a Check Point network object:
   - Choose Manage > Network Objects > New > Check Point > Host from the menu. The Check Point Host window is displayed.
   - In the General Properties page, define the standard network object properties, including:
     - Checking Log Server in the Check Point Products list.
     - Setting up Secure Internal Communication between this Log Server and the Security Management server.
   - Define additional properties as needed and click OK.

3. Install the Check Point Objects Database on the Log Server object:
Choose **Policy > Install Database** from the menu. The **Install Database** window is displayed.

In the Install Database on list, check the Log Server object and click OK.

4. To setup the gateway to forward its logs to this Log Server, double-click the gateway so that its properties window is displayed.

5. You can either forward the log records **online**, one by one; or save the records locally, and then forward them in a **file** according to a specific schedule.

**To forward log records online:**
- Display the **Log Servers** page (under the **Logs and Masters** branch).
- Check **Define Log Servers**.
- Add this Log Server to the **Always send logs to** table (click **Add** to display the **Add Logging Servers** window, and move the Log Server from the **Available Log Servers** list to the **Select Log Servers** list).

**To specify a log file forwarding schedule:**
- Display the **Additional Logging Configuration** page (under the **Logs and Masters** branch).
- In the **Log forwarding settings** section, set the following:
  - Check **Forward log files to Log Server** and choose the Log Server from the drop-down list.
  - Set a **Log forwarding schedule** by choosing the appropriate time object from the drop-down list.

6. By default, when the selected Log Server is unreachable, the logs are written to a local file. Alternatively, you can select a **backup** Log Server as follows:
- Display the **Log Servers** page (under the **Logs and Masters** branch).
- Under **When a Log Server is unreachable, send logs to section**, click **Add** to display the **Add Logging Servers** window.
- Move the Log Server from the **Available Log Servers** list to the **Select Log Servers** list and click **OK**.

7. Repeat **step 4 to step 6** on all relevant gateways.

8. Launch SmartView Tracker and login to this Log Server (instead of the Security Management server).

### Custom Commands

**To configure the commands you can run through SmartView Tracker:**

1. Choose **Tools > Custom Commands** from the menu. The **Custom Commands** window is displayed.
2. Click **Add**. The **Add New Command** window is displayed.
3. Specify the following command properties:
   - **Menu Text**, defines how this command is to be displayed in the right-click menu (e.g. **Ping**).
   - **Command**, specifying the name of the command (e.g. **ping.exe**).
   - **Arguments** to be used by the command.
   - **IP Columns only**, allowing you to apply this command only to columns that have an IP address value (e.g. Origin, Source, Destination etc.).

   **Note** - It is recommended not to use a full path name in the Executable field, since the executable file may be found in different directories of different SmartView Tracker clients. The administrator must ensure that the command can be executed from the SmartView Tracker installation directory. Commands requiring a full path can be executed by a script, which all administrators save in the same directory, but each administrator edits according to his or her needs.

**Example:**

1. Use the **Add New Command** window to add the **Menu Content TELNET**, which runs the command **TELNET** using **<Cell Value>** as its **Parameter**.
2. In the **Records** pane, right-click a record whose IP address is 20.13.5.2. and select telnet from the menu.
   The executed command is: `telnet 20.13.5.2`.

### Block Intruder

SmartView Tracker allows you to terminate an active connection and block further connections from and to specific IP addresses. The Block Intruder feature only works on UDP and TCP connections. Proceed as follows:

1. Select the connection you wish to block by clicking it in the **Active** mode's **Records** pane.
2. From the **Tools** menu, select **Block Intruder**.
   The **Block Intruder** window is displayed.
3. In **Blocking Scope**, select the connections that you would like to block:
   - **Block all connections with the same source, destination and service** - block the selected connection or any other connection with the same service, source or destination.
   - **Block access from this source** - block access from this source. Block all connections that are coming from the machine specified in the Source field.
   - **Block access to this destination** - block access to this destination. Block all connections that are headed to the machine specified in the Destination field.
4. In **Blocking Timeout**, select one of the following:
   - **Indefinite** blocks all further access
   - **For x minutes** blocks all further access attempts for the specified number of minutes
5. In **Force this blocking**, select one of the following:
   - **Only on** blocks access attempts through the indicated Security Gateway.
   - **On any Security Gateway** blocks access attempts through all Security Gateways defined as gateways or hosts on the Log Server.
6. Click **OK**.
   To clear blocked connections from the display, choose **Clear Blocking** from the **Tools** menu.

### Configuring Alert Commands

When you set a rule's **Track** column to **Alert**, **SNMP Trap**, **Mail** or **UserDefined**, a log of the event matching the rule is written to the active log file and the Security Management server executes the appropriate alert script.

Alert scripts are defined through the SmartDashboard, in the **Global Properties** window's **Alert Commands** page. You can use the default mail alert and SNMP trap alert scripts, by entering the appropriate IP addresses. Alternatively, define your own alert(s) in the three **UserDefined** fields.

### Enable Warning Dialogs

When working with SmartView Tracker, messages will appear in a variety of situations. Some of these messages have the option "Don't show this dialog box again". The **Tools > Enable Warning Dialogs** enables you to view all the dialog boxes for which you selected "Don't show this dialog box again".
Chapter 6

Identity Logging

In This Chapter

Introduction 86
Configuration 89
Troubleshooting 92

Introduction

This feature enhances activity tracking by incorporating user and computer identification information into the Check Point logs. When analyzing network traffic and security-related events, it is important to identify the specific user and computer that generates traffic. Typically, source traffic is identified only by its URL or IP address.

Security Management extracts user and computer name information from Active Directory (AD) logs and inserts this information into the Check Point logs. This additional information augments the audit trail provided by Check Point tools such as Event Correlation, SmartEvent Intro and SmartReporter.

The addition of user and computer identity information plays a key role in:

- Security auditing
- Troubleshooting network and connectivity issues
- Help desk and maintenance tasks
- Compliance and policy enforcement

To use Identity Logging, you must have a license for the Logging and Status Software Blade installed on the Security Management Server or Provider-1 MDS.

How it Works

User and computer identification information is obtained from Active Directory logs and is stored in an association map on the log server. When network or security activity generates a Check Point log entry, the log server obtains the user and computer name from the association map entry corresponding to the source IP address. If there is no entry in the association map corresponding to the source IP address, no user identification information is added to the log entry.

The log server automatically creates an entry in association map when it receives an AD log entry for a given IP address from the domain controller. While this association remains active, the log server adds the user and/or computer name associated with the designated IP address to Check Point logs.
The following example illustrates this process:

**Figure 6-12**  Identity Logging workflow

1. An Active Directory transaction, such as a user logging on to the domain, generates an AD log entry for IP 10.10.10.1.
2. The AD Log, containing the user name, computer name and IP address is transmitted to the log server. This action creates an entry in the association map that associates the IP address with a specific user name and computer name.
3. This same user surfs to a blocked website.
4. The security policy drops the traffic and generates a Check Point log entry for IP 10.10.10.1.
5. The log server obtains the user and computer name from the association map entry corresponding to IP 10.10.10.1, which then appears in SmartView Tracker.

   **Note** - The above example describes a scenario using identity data for the source IP address. Identity logging works equally well with identity data for the destination IP address.

Communication between the log server and the Active Directory domain controllers is handled by the *Windows Management Instrumentation (WMI)* protocol. WMI is enabled by default on Active Directory domain controllers.

You configure Identity Logging using SmartDashboard on your management servers. No WMI or domain controller configuration is required to enable Identity Logging.

### How an Association Expires

An association automatically expires under the following conditions:

- After an administrator-defined interval, during which no further AD log entries are received for that IP address.
- If the log server receives another AD log entry that associates the IP address with different computer.

   **Note** - An association does not expire if another AD log entry is received that associates an existing IP address with another user name. In this case, both user names appear in Check Point log entries until they expire as explained above.
Log Contents

The following examples demonstrate how user and computer identification information appear in SmartView Tracker logs.

<table>
<thead>
<tr>
<th>No.</th>
<th>Date</th>
<th>Time</th>
<th>User Name</th>
<th>Source</th>
<th>Source User Name</th>
<th>DestIP</th>
<th>Rule</th>
<th>Current Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>120146</td>
<td>12Nov2009</td>
<td>19:20:45</td>
<td>nhname</td>
<td>ZEONXON</td>
<td><a href="mailto:administrator@nxy.com">administrator@nxy.com</a></td>
<td>10.13.180.255</td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120147</td>
<td>12Nov2009</td>
<td>19:20:45</td>
<td>nhname</td>
<td>ZEONXON</td>
<td><a href="mailto:administrator@nxy.com">administrator@nxy.com</a></td>
<td>10.13.180.255</td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120148</td>
<td>12Nov2009</td>
<td>19:22:47</td>
<td>domain... tam</td>
<td>tam</td>
<td><a href="mailto:tam@nxy.com">tam@nxy.com</a></td>
<td>gsint-checkaps</td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120152</td>
<td>12Nov2009</td>
<td>19:25:58</td>
<td>domain... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120153</td>
<td>12Nov2009</td>
<td>19:25:58</td>
<td>domain... 398</td>
<td>398</td>
<td>NEWPC</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120154</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120155</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120156</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120157</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120158</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120159</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120160</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120161</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120162</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
<tr>
<td>120163</td>
<td>12Nov2009</td>
<td>19:25:59</td>
<td>Kerberos... NEWPC</td>
<td>NEWPC</td>
<td>Hez_Hannan0000</td>
<td><a href="mailto:ipnoc@nxy.com">ipnoc@nxy.com</a></td>
<td>1</td>
<td>1-Standard</td>
</tr>
</tbody>
</table>

Hardware Requirements

The following table lists supported platforms for the Security Management/log server and Active Directory domain controller.

<table>
<thead>
<tr>
<th>Component</th>
<th>Supported Platforms</th>
</tr>
</thead>
</table>
Configuration

You configure User and Computer Identification settings using SmartDashboard on any Security Management Server or log server object.

Note - The Security Management Server must have a Logging and Status Software Blade license installed, and the Software Blade must be enabled on the Security Management Server network object.

Configuring the Firewall

If a Security Gateway is located between the Log server and the Active Directory controller, configure the Firewall to allow WMI traffic.

To create firewall rules for WMI traffic:

1. In SmartDashboard > Firewall, create a rule that allows ALL_DCE_RPC traffic:
   - Source and Destination = Domain Controllers, management servers, and log servers
   - Service = ALL_DCE_RPC
   - Action = Accept

2. Save the policy and install it on Security Gateways.

Note - If there are connectivity issues on DCE RPC traffic after this policy is installed, see sk37453 (http://supportcontent.checkpoint.com/solutions?id=sk37453) for a solution.

Configuring Identity Logging

Configure the Security Management Server, Provider-1 CMAs, and Log Servers to enable them to be used with Active Directory mappings.

To configure a server for Identity Logging:

1. In SmartDashboard, double-click an existing server object.
2. Select Logs and Masters > User Identification.
3. In the **User Identification** window, configure the following settings:

![Configuration window](image)

a) **Enable display of user and computer names based on Active Directory mappings**: Enable this option to include user and computer identity information in Check Point log entries.

b) **Create log entry when User or machine associations are created or expire**: Enable this option to create a Check Point log entry each time an user/IP association is created or expires.

c) **Domain Name**: Enter the Active directory domain name.
   - **Domain Controllers**: Add domain controllers to monitor for Active Directory log retrieval. You should add all domain controllers that users may connect to. Click **Add** and select a domain controller to add it to the list of monitored domain controllers.
   - Click **Edit** to modify configuration settings for the selected domain controller.
   - Click **Remove** to remove the selected domain controller from the list of monitored domain controllers.

d) **Active Directory administrator credentials**: Enter the Active Directory administrator user name and password. Click **Test** to verify that the supplied credentials successfully gain access to the domain controller.

   **Important** - The domain administrator credentials are used only to receive AD security logs and the full user name from the remote domain controllers.

   Under no circumstances do these actions modify any AD data, including the security logs.

e) **Advanced**: Click to open the **Advanced Configuration** window. This window allows you to set the association timeout period and to exempt specific users and networks from Identity Logging.
Configuring Advanced Settings

In the Advanced Configuration window, configure the following settings:

- **IP/User Association Timeout**: Enter the time, in minutes, after which the association between the user, computer and IP address automatically expires.

- **Ignored Users**: Enter specific users for which user and computer identify information is not logged. For example, you may wish to exclude 'dummy' user names used for automatic actions or services running on endpoint computers (anti-virus, backup, etc.). You can also use the * wildcard character to specify multiple users.

- **Excluded Networks**: Select specific networks for which user and computer identify information is not logged. For example, you may wish to exclude lab networks or test beds. Click Add and then select a network or networks to exclude from Identity Logging.

Completing Configuration

After configuring Identity Logging for a Security Management Server or Provider-1 CMA, you must re-install the database. Without this step, Identity Logging will not function.

**To install the database:**

1. Select Policy > Install Database...

   The Install Database window appears.

2. Select the machine(s) on which you would like to install the database and click OK.

   The Install Database script appears.

3. Click Close when the script is complete.

Optimizing Identity Logging

The following tips can help optimize your use of Identity Logging and minimize the performance impact caused by its use.

- Restrict Active Directory log monitoring to relevant domain controllers, eliminating non-essential traffic.

- Avoid monitoring remote domain controllers.

- Exclude non-essential users, such 'dummy' users used for automated transactions from identification logging.
• Exclude specific high-volume users from identification logging. Such users are often easy to identify by other log information.
• Exclude lab, test bed, and other non critical networks from identification logging.

Troubleshooting

If you experience connectivity problems between your domain controllers and management/log servers, perform the following troubleshooting steps:

In this section:

Install Database 92
Use wbemtest to Verify WMI 92
Check Connectivity 93
Check Domain Administrator Credentials 93
Verify the WMI Service 93

Install Database

Before continuing more sophisticated troubleshooting procedures, check this:

If you have configured Identity Logging, but do not see identities in logs, make sure you installed the database ("Completing Configuration" on page 91).

Use wbemtest to Verify WMI

To use the Microsoft wbemtest utility to verify that WMI is functional and accessible.

1. Click Start > Run.
2. Enter wbemtest.exe in the Run window.
3. In the Windows Management Instrumentation Tester window, click Connect.
4. In the Connect window, enter the following information:

   a) Domain controller in the following format: \\
      <IP address>\root\cimv2
   
   For example: \\
   \11.22.33.44\root\cimv2
5. Click Connect.

6. If the Windows Management Instrumentation Tester window re-appears with its buttons enabled, WMI is fully functional.

7. If the connection fails, or you receive an error message, check for the following conditions:
   a) Connectivity ("Check Connectivity" on page 93) problems
   b) Incorrect domain administrator credentials ("Check Domain Administrator Credentials" on page 93).
   c) WMI service ("Verify the WMI Service" on page 93) is not running
   d) A firewall is blocking traffic ("Configuring the Firewall" on page 89) between the log server and domain controller.

Check Connectivity
1. Ping the domain controller from the log server.
2. Ping the log server from your management server.
3. Perform standard network diagnostics as required.

Check Domain Administrator Credentials
To verify your domain administrator credentials:
1. Click Start > Run.
2. Enter \<domain controller IP>\c$ in the Run window. For example For example: \\
11.22.33.44\c$.
3. In the Logon window, enter your domain administrator user name and password.
4. If the domain controller root directory appears, this indicates that your domain administrator account has sufficient privileges. An error message may indicate that:
   a) If the user does not have sufficient privileges, this indicates that he is not defined as a domain administrator. Obtain a domain administrator's credentials.
   b) You entered the incorrect user name or password. Check and retry.
   c) The domain controller IP is incorrect or you are experiencing connectivity issues.

Verify the WMI Service
To verify if the WMI service is running:
1. Click Start > Run.
2. Enter services.msc in the Run window.
3. Locate the Windows Management Instrumentation service and verify that the service has started.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Status</th>
<th>Startup Type</th>
<th>Log On As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows CardSpace</td>
<td>Securely e...</td>
<td>Manual</td>
<td>Local System</td>
<td>Local System</td>
</tr>
<tr>
<td>Windows Driver Foundation - User-mode Driver Fr...</td>
<td>Manages u... Started Automatic Local System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Firewall/I...</td>
<td>Provides i... Started Automatic Local System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Image Acquis... (WIA)</td>
<td>Provides i... Manual Manual Local System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Installer</td>
<td>Add, mod... Manual Manual Local System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td>Provides a... Started Automatic Local System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation Driver Exte...</td>
<td>Provides s... Manual Manual Local System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Media Player Network Share...</td>
<td>Shares Win... Manual Network S...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Presentation Foundation Font Cache 3.0.0.0</td>
<td>Optimizes ... Manual Manual Local Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Time</td>
<td>Maintains d... Started Automatic Local System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wired AutoConfi...</td>
<td>This ser... Started Automatic Local System</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If it has not started, right-click this service and select Start from the option menu.
Chapter 7

Policy Backup and Version Control

In This Chapter

The Need for Security Management 94
The Security Management Solution 94

The Need for Security Management

The Security Management server is the security center of the organization. Changes that are made in the Security Management server must be completely secure and efficient in order to avoid even the most temporary compromise of the system.

Organizations are dynamically shifting all the time. Network security needs to be maintained constantly, and occasionally certain modifications are necessary, such as updating the Security Policy and Check Point software.

When modifications need to be made to the network, you must ensure that backups are available and in place. These backups are usually replicas of the functioning environment which can be used if the changes are not applied successfully. In other words, it is possible to use backups in order to revert to the version of the network as it was before the significant changes were applied. There may also be legal reasons which compel companies to maintain backup versions.

By taking precautions prior to making changes to the Security Policy, the system administrator can make extra sure that all the conditions necessary for a smooth, seamless upgrade operation exist. Although it is possible to perform a live upgrade on a Security Management server, it is advisable to prepare an upgraded machine which can be examined carefully to ensure that it is functioning properly. Once it is certain that this upgraded machine is working properly, it can slowly be integrated in place of the existing Security Management server. Under these circumstances, information can be exported to the upgraded machine from the original machine without any problems.

The Security Management Solution

General

The Security Management server has several tools which allow changes in the production environment to be made securely, smoothly and efficiently. These include:

- Revision control – the Security Management server can manage multiple versions of policies. Different versions of policies can be stored and viewed using the Revision control tool. This tool enables the system administrator to revert the current policy to a previously saved version. For more information, see Managing Policy Versions (on page 95).

- Backup & Restore – when it is imperative that the Security Management server be upgraded, it is possible to create a functioning Security Management server which will replace the existing machine while it is being serviced. This Backup server is an upgraded clone of the existing Security Management server. The system administrator tests it in order to ensure that it is fully functioning and thereafter integrates it in place of the original Security Management server. For more information, see Backup and Restore the Security Management server (on page 97).
Managing Policy Versions

Policies are created by the system administrator and managed via the Security Management server. Different versions of these policies can be saved. Each version includes backups of the various databases (objects, users, Certificate Authority data, etc.). This information is zipped and saved.

The existing versions are recorded in a “Version table”. This table can be viewed and the versions which are displayed can be modified. It is possible to:

- Create a Version
- Export and Import a Version (on page 95)
- View a Version (on page 95)
- Revert to a Previous Version (on page 95)
- Delete a Version (on page 96)

Versions can be created manually by the system administrator, or the system can be set to automatically create a new version every time Security Policy installation takes place.

Version Operations

The following operations can be executed for version control:

Create a Version

A new version can be created manually by the system administrator, or the system can be set to create new versions automatically every time a new policy is installed. Each new version has the following attributes:

- the creation date
- the system administrator who initiated the new version
- the version of the software
- three editable options determined by the system administrator:
  - the name of the version
  - an additional optional comment
  - a checkbox you can select if you want to ensure that this version will not be automatically deleted (if the automatic deletion of database revisions is activated)

Note - It is recommended to create a version before upgrading the system. This enables the administrator to back out to a functioning environment in case of problems during the upgrade operation.

Export and Import a Version

It is possible to export existing versions using the Command Line. This can be useful in order to save disk space. When the exported version is necessary, it can be imported back into the Versions table. The imported version appears in the version table as a regular maintained version.

View a Version

A saved version can be viewed in SmartDashboard. For every saved version you can view certain entities such as objects, users, rules. Various operations, such as queries can be executed on these entities.

Revert to a Previous Version

The revert operation allows you to revert to a previously saved version. Once you initiate the revert operation, the selected version overwrites the current policy. The one type of information that is not
overwritten, is Certificate Authority (CA) data. For security reasons, CA data is not overwritten, but it is merged with the CA data of the current policy.

Before the revert operation is done, the system administrator can expect to receive a report on the expected outcome of the revert operation. For example, information certificates that are going to be revoked is supplied. At this point it is necessary for the system administrator to decide whether or not to continue with the revert operation. Of all the entities included in the reverted version, the user database is not automatically reverted. This is because the users database is extremely dynamic; users are added and deleted frequently. The user database is always changing regardless of the policy version. The system administrator can decide to revert to a selected Policy version, but to maintain the current users database. In this manner, the current user base is used with the restored Policy.

Delete a Version

A previously saved version can be deleted. This operation will also delete the various databases included in the policy version.

Version Configuration

Version Operations are performed via the Database Revision Control window. This window can be accessed by selecting File > Database Revision Control.

In this window you can:

- Create a new version of the current policy manually by clicking Create. When automatic deletion of database versions is activated, you can specify here whether to keep the given version to ensure that it will not be deleted automatically.
- View a saved version by clicking Action > View Version.
- Revert to a saved version by clicking Action > Restore Version.
- View the SmartWorkflow Summary of Changes report, which compares the previous policy installation with the currently pending policy installation by clicking Action > Compare Versions.
- View the properties of a selected version by clicking Properties. Certain of the version options are editable.
- Delete a selected version by clicking Delete.
- Configure settings for automatic deletion of database versions by selecting the Automatically delete old versions checkbox and clicking Configure.

Configure Automatic Deletion

You can configure how to automatically delete old database versions by selecting one of the four radio button options:

- **Delete versions older than: X versions** - where X represents the number of most recent versions that should be kept and all versions older than that should be deleted. The default is 50.
- **Delete versions older than: X days** - where X represents the time period from today backwards for which all versions created during that time frame should be kept and all versions older than that should be deleted.
- **Delete oldest versions when version storage exceeds: X MBs/Percent** - where X specifies the maximum allowed total of MB of storage space allocated for all database versions. Alternatively, a percentage from the total disk space can be specified. Upon reaching the limit, the oldest versions are deleted.
- **Delete oldest versions when available disk space is less than: X MBs/Percent** - where X specifies the minimum allowed available free disk space in MBs or a percent value. When this limit is reached, the oldest versions are deleted.

>Note - SmartWorkflow versions are not affected by this feature. They are neither counted nor deleted.
Version Upgrade

When the Security Management server is upgraded, the various versions are upgraded as well. This means that saved versions will be compliant with the upgraded software, and there will not be a need to downgrade to a previous software version in order to revert to a saved version. For example, new object attributes are added to comply with the new features.

Version Diagnostics

The success or failure of version operations that require modification of the Versions table (such as creating, reverting to or deleting a version) are audited in the audit log of the SmartView Tracker. It is recommended to make use of these logs to ensure that operations have taken place successfully.

Saved versions require disk space. If the existing disk space is exhausted, a threshold alert is sent to the SmartView Monitor. Use this SmartConsole in order to make sure that you meet the disk space requirements needed to implement the versioning feature.

Manual versus Automatic Version Creation

It is possible to create a new version of the current policy by clicking Create in the Database Revision Control window.

Alternately, new versions can be configured to be created automatically every time a policy is installed. You can do this by selecting Create new version upon install policy operation in the Install Policy window. You can access this window by selecting Policy > Install.

Backup and Restore the Security Management server

The Backup and Restore operation exports the Security Management server environment from the Security Management server, and allows it to be imported to another machine. This other machine is a working clone of the Security Management server. It has identical functionalities and capabilities as the original Security Management server. This operation supports Operating System (OS) migration, meaning that the OS of the original, as well as the clone machines can be different.

Using the Backup and Restore feature it is possible to:

- Replace the original Security Management server with another clone Security Management server, while the original is being serviced.
- Maintain a backup of the Security Management server to be used in case of failover.
- Upgrade the Security Management server. System administrators are cautious when upgrading the Security Management server in the production environment. It is more secure to upgrade another machine, import the information from the original Security Management server in order to make a clone. Once the clone has been tested thoroughly and it is found to be fully functional, it can be integrated as the official Security Management server operating in the production environment. The imported information is upgraded prior to being integrated into the new machine so that it complies with the new and/or changed features relevant to the software version to which the Security Management server has been upgraded.
## Chapter 8

### Management Portal

In This Chapter

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Management Portal</td>
<td>99</td>
</tr>
<tr>
<td>Deploying the Management Portal on a Dedicated Server</td>
<td>99</td>
</tr>
<tr>
<td>Deploying the Management Portal on the Security Management server</td>
<td>99</td>
</tr>
<tr>
<td>Management Portal Configuration and Commands</td>
<td>100</td>
</tr>
<tr>
<td>Client Side Requirements</td>
<td>100</td>
</tr>
<tr>
<td>Connecting to the Management Portal</td>
<td>101</td>
</tr>
<tr>
<td>Using the Management Portal</td>
<td>101</td>
</tr>
<tr>
<td>Troubleshooting Tools</td>
<td>101</td>
</tr>
</tbody>
</table>
Overview of Management Portal


The product can be deployed on a dedicated server, or alongside the Security Management server. SSL encrypted connections are used to access the Management Portal web interface. Administrative access can be limited to specific IP addresses. Dedicated administrator users can be limited to Management Portal access only.

In This Document

Deploying the Management Portal on a Dedicated Server 99
Deploying the Management Portal on the Security Management server 99
Management Portal Configuration and Commands 100
Client Side Requirements 100
Connecting to the Management Portal 101
Using the Management Portal 101
Troubleshooting Tools 101

Deploying the Management Portal on a Dedicated Server

When deploying the Management Portal on a dedicated server, the following actions should be taken to successfully integrate the Management Portal Server with the Security Management server.

1. During the Management Portal installation you will be asked to choose a SIC (Secure Internal Communication) password that will be used to establish trust with the Security Management server.

   - Fill in the network objects properties.
   - Select Management Portal from the Management tab of the Software Blades list.

3. Add access rules to allow administrative access to the Management Portal Server.

4. Create administrator users with Management Portal permissions if you want to restrict access to the Management Portal.
   - Administrator users can be limited to Management Portal access only using a Permission profile.
     Create a Permission profile by selecting the Allow access via Management Portal only permission for the specific administrator.

Deploying the Management Portal on the Security Management server

When deploying the Management Portal alongside the Security Management server, the following actions should be taken to successfully integrate the Management Portal component with the Security Management server.

1. Modify the Security Management server network object to include the Management Portal in its Software Blades list if the Management Portal was installed after the Security Management server. If the Management Portal and the Security Management server were installed from the same wrapper this step is unnecessary.

2. Add access rules to allow administrative access using TCP 4433 to the Security Management server itself.
3. Create administrator users with Management Portal permissions if you want to restrict access to the Management Portal.
   - Administrator users can be limited to Management Portal access only using a Permission profile. Create a Permission profile by selecting the **Allow access via Management Portal only** permission for the specific administrator.

**Management Portal Configuration and Commands**

**Management Portal Commands**

- **smartportalstop**: Stops Management Portal services.
- **smartportalstart**: Starts Management Portal services.

**Limiting Access to Specific IP Addresses**

To allow only specific IP addresses or networks to access the Management Portal, stop the Management Portal and create the `hosts.allow` file under the Management Portal `conf` directory (in Windows: `C:\program files\CheckPoint\R71\SmartPortal\portal\conf` and in Solaris, Linux and SecurePlatform: `/opt/CPportal-R71/portal/conf`). If the `hosts.allow` file is not in the Management Portal `conf` directory you should create it if it is required.

The file format is:

- ALL: ALL (to allow all IPs)
- ALL: x.x.x.x (to allow specific IPs)
- ALL: x.x.x.x/y.y.y.y (to allow specific networks where x.x.x.x is the IP address and y.y.y.y is the netmask)

**Management Portal Configuration**

The following Management Portal product properties can be modified by editing the `cp_httpd_admin.conf` file. This file can be found in the Management Portal `conf` directory.

- **Note** - Any modifications to the `cp_httpd_admin.conf` file should be done after performing `SmartPortalStop`.

- To change the web server port, modify the `PORT` attribute (default is TCP 4433).
- To use HTTP instead of HTTPS set the SSL attribute to 0. It is not recommended to do this for security reasons and should only be used when troubleshooting.
- To change the Web Server certificate modify the `SERVCERT` (the full path to the certificate) and `CERTPWD` (the certificate password) attributes.

**Client Side Requirements**

The Management Portal can be used with the following web browsers:

- Internet Explorer
- Mozilla
- FireFox
- Netscape
The Management Portal requires that you enable JavaScript and disable Popup blockers in your browser.

**Connecting to the Management Portal**

Connect to the Management Portal by opening one of the supported browsers and pointing it to:


**Using the Management Portal**

Once you have authenticated, click on the HELP button to display the Management Portal Online Help. The Online help explains the functionality of each window.

**Troubleshooting Tools**

- The web demon (cpwmd) error log file is `cpwmd.elg` and can be found in the Management Portal log (in Windows: `C:\program files\CheckPoint\R71\SmartPortal\portal\log` and in Solaris, Linux and SecurePlatform: `/opt/CPportal-R71/portal/log`) directory.
- The web server (cp_http_server) error log file is `cphttpd.elg` and can be found in the Management Portal log directory.

  - To see debug cpwmd messages perform the following:
    - `cpwmd debug -app the Management Portal` on
  
  - To see debug cpwmd messages with greater detail perform the following:
    - `cpwmd debug -app SmartPortal` on **TDERROR_ALL_ALL=5**

  - To see additional cp_http_server debug messages you should stop the daemon using `cpwd_admin stop -name CPHTTPD` and perform the following:
    - set the **TDERROR_CPHTTPD_ALL** environment variable to 5.
    - set the **OPSEC_DEBUG_LEVEL** environment variable to 3.
    - execute `cp_http_server -v -f <full path to the cp_httpd_admin.conf file>`.

  - To see CGI log messages of incoming and outgoing data, you should stop the `cp_http_server` daemon, set the **CFWM_DEBUG** environment variable to 1 and run `cp_http_server`.

  - The output will be written to the `cgi_log.txt` and `cgi_out.txt` files in the temp directory (`c:\temp` on Windows and `/tmp` on Unix/Linux/SPLAT).
Chapter 9

SmartUpdate

In This Chapter

The Need for Software Upgrade and License Management 102
The SmartUpdate Solution 102
Upgrading Packages 105
Managing Licenses 109
Service Contracts 113
Generating CPInfo 113
The SmartUpdate Command Line 114

The Need for Software Upgrade and License Management

Managing remote Security Gateways can be time-consuming and difficult. Keeping remote firewalls and gateways up-to-date with the latest security patches and software often requires expertise on-site, an expensive proposition when managing dispersed networks. Even in small local networks, the routine of applying patches and distributing licenses can tax an organization's technical resources.

The SmartUpdate Solution

Introducing SmartUpdate

SmartUpdate automatically distributes applications and updates for Check Point and OPSEC Certified products, and manages product licenses. It provides a centralized means to guarantee that Internet security throughout the enterprise network is always up to date. SmartUpdate turns time-consuming tasks that could otherwise be performed only by experts into simple point and click operations.

SmartUpdate extends your organization's ability to provide centralized policy management across enterprise-wide deployments. SmartUpdate can deliver automated software and license updates to hundreds of distributed security gateways from a single management console. SmartUpdate ensures security deployments are always up-to-date by enforcing the most current security software. This provides greater control and efficiency while dramatically decreasing maintenance costs of managing global security installations.

SmartUpdate enables remote upgrade, installation and license management to be performed securely and easily. A system administrator can monitor and manage remote gateways from a central location, and decide whether there is a need for software upgrade, new installations and license modification. It is possible to remotely upgrade:

- Check Point Security Gateways
- Hotfixes, Hotfix Accumulators (HFAs) and patches
- Third party OPSEC applications
- UTM-1 Edge
- Check Point IPSO Operating System
Understanding SmartUpdate

SmartUpdate installs two repositories on the Security Management server:

- **License & Contract Repository**, which is stored on all platforms in the directory `$FWDIR\conf\`.
- **Package Repository**, which is stored:
  - on Windows machines in `C:\SUroot`.
  - on UNIX machines in `/var/suroot`.

The Package Repository requires a separate license, in addition to the license for the Security Management server. This license should stipulate the number of nodes that can be managed in the Package Repository.

Packages and licenses are loaded into these repositories from several sources:

- the Download Center web site (packages)
- the Check Point CD (packages)
- the User Center (licenses)
- by importing a file (packages and licenses)
- by running the `cplic` command line

Of the many processes that run on the Check Point Security Gateways distributed across the corporate network, two in particular are used for SmartUpdate. Upgrade operations require the `cprid` daemon, and license operations use the `cpd` daemon. These processes listen and wait for the information to be summoned by the Security Management server.

From a remote location, an administrator logged into the Security Management server initiates operations using the SmartUpdate tool. The Security Management server makes contact with the Check Point Security Gateways via the processes that are running on these gateways in order to execute the operations initiated by the system administrator (e.g., attach a license, or upload an upgrade). Information is taken from the repositories on the Security Management server. For instance, if a new installation is being initiated, the
information is retrieved from the Package Repository; if a new license is being attached to remote gateway, information is retrieved from the License & Contract Repository.

This entire process is Secure Initial Communication (SIC) based, and therefore completely secure.

SmartUpdate - Seeing it for the First Time

SmartUpdate has two tabs:

- **Packages** tab shows the packages and Operating Systems installed on the Check Point Security Gateways managed by the Security Management server. Operations that relate to packages can only be performed in the Packages tab.

- **Licenses** tab shows the licenses on the managed Check Point Security Gateways. Operations that relate to licenses can only be performed in the Licenses tab.

These tabs are divided into a tree structure that displays the packages installed and the licenses attached to each managed Security Gateway.

The tree has three levels:

- Root level shows the name of the Security Management server to which the GUI is connected.

- Second level shows the names of the Check Point Security Gateways configured in SmartDashboard.

- Third level shows the Check Point packages (in the Packages tab) or installed licenses (in the Licenses tab) on the Check Point Security Gateway.

Additionally, the following panes can be displayed:

- **Package Repository** - shows all the packages available for installation. To view this pane, select Packages > View Repository.

- **License & Contract Repository** - shows all licenses (attached or unattached). To view this pane, select Licenses > View Repository.

- **Operation Status** - shows past and current SmartUpdate operations. To view this pane, select Operations > View Status. In this pane you can read about:
  - Operations performed (e.g., Installing package <X> on Gateway <Y>, or Attaching license <L> to Gateway <Y>).
  - The status of the operation being performed, throughout all the stages of its development (for instance, operation started, or a warning).
  - A progress indicator.
  - The time that the operation takes to complete.

Common Operations

**Dragging and Dropping**

Packages and licenses can be dragged and dropped from the Repositories onto the Security Gateways in the Package/Licenses Management tree. This drag and drop operation will invoke the distribute or attach operation respectively.

**Sorting**

To sort in ascending or descending order, click the column title in the Licenses or Packages tab.

**Expanding or Collapsing**

To expand or collapse the Check Point Security Gateways tree structure, right-click on the tree root and choose Expand/Collapse.
**Modifying the Repository View**

Modify the Repository View as follows:

1. Right-click on a blank row or column in the Repository window
2. Select one of the options. For instance, in the Licenses Repository you can select to view only the attached licenses, whereas, in the Packages Repository, you can select to view certain packages, like the available OS packages.

**Clearing the Repository of Completed Operations**

To clear a single operation, select the line in the Operation Status window and press the Delete key, or right-click and select Clear.

To clear all completed operations from the Operation Status window, select Status > Clear all completed operations.

**Viewing Operation Details**

To view operation details, in the Operation Status window, double-click the operation entry. The Operation Details window shows the operation description, start and finish times, and progress history. The window is resizable.

To copy the Status lines to the clipboard, select the line, right-click and choose Copy.

**Searching for Text**

To search for any text string: select Tools > Find. The Find window is displayed.

- Enter the string for which you would like to search in the Find what field.
- Select where you would like to search, e.g., License & Contracts tab or Package Repository.

**Printing Views**

To print a view, select File > Print. The Choose Window is displayed. Select the window that you would like to print, e.g., Operation Status or License & Contract Repository. Optionally, you can adjust the print setup settings, or preview the output.

**Logging SmartUpdate Operations**

- A log file of SmartUpdate package operations is generated in the file $SUROOT\log\su.elg.
- An audit log of SmartUpdate operations can be viewed in the SmartView Tracker Audit View.

**Upgrading Packages**

**Overview of Upgrading Packages**

The latest management version can be applied to a single Check Point Security Gateway, or to multiple Check Point Security Gateways simultaneously. Use the Upgrade all Packages operation to bring packages up to the most current management version.

When you perform Upgrade all Packages all products are upgraded to the latest Security Management server version. This process upgrades both the software packages and its related HFA (that is, the most up to date HFA is installed). Once the process is over, the software packages and the latest HFA will exist in the Package Repository.

To upgrade Check Point packages to versions earlier than the latest available version, they must be upgraded one-by-one. Use the Distribute operation to upgrade packages to management versions other than the most current, or to apply specific HFAs.
In addition, SmartUpdate recognizes gateways that do not have the latest HFA. When you right-click an HFA in the Package Repository and select Distribute for that specific HFA, you will receive a recommendation to install a new HFA on the gateways that do not have it.

The Upgrade Package Process

Prerequisites for Remote Upgrades

- Ensure that SmartUpdate connections are allowed. Go to SmartDashboard > Policy > Global Properties > FireWall Implied Rules, and ensure that the Accept SmartUpdate Connections check box is checked.
- Secure Internal Communication (SIC) must be enabled to allow secure communications between the Security Management server and remote Check Point Security Gateways.

Retrieving Data From Check Point Security Gateways

In order to know exactly what OS, vendor and management version is on each remote gateway, you can retrieve that data directly from the gateway.

- To retrieve data on a specific Check Point Security Gateway, right-click on the gateway in the Package Management window and select Get Gateway Data.
- If you are installing or upgrading multiple Check Point Security Gateways, from the Packages menu select Get Data From All.

Adding New Packages to the Package Repository

To distribute (that is, install) or upgrade a package, you must first add it to the Package Repository. You can add packages to the Package Repository from the following three locations:

Download Center

1. Select Packages > New Package > Add from Download Center.
2. Accept the Software Subscription Download Agreement.
3. Enter your user credentials.
4. Select the packages to be downloaded. Use the Ctrl and Shift keys to select multiple files. You can also use the Filter to show just the packages you need.
5. Click Download to add the packages to the Package Repository.

User Center

Use this procedure for adding OPSEC packages and Hotfixes to the Package Repository.
1. Open a browser to the Check Point Support Center (http://supportcenter.checkpoint.com).
2. Select the package you want to upgrade.
3. Enter your user credentials.
4. Accept the Software Subscription Download Agreement.
5. Choose the appropriate platform and package, and save the download to the local disk.
7. In the Add Package window, navigate to the desired .tgz file and click Open to add the packages to the Package Repository.

Check Point CD

1. Select Packages > New Package > Add from CD.
2. Browse to the location of the CD drive, and click OK. The Add Package From CD window opens, showing the available packages on the CD. (If you wish to upload packages from the Check Point Comprehensive CD, select the CD-Rom drive as the path.)
3. Select the package(s) to be added to the Package Repository (Ctrl-select for more than one package), and click OK.
Verifying the Viability of a Distribution

Verify that the distribution (that is, installation) or upgrade is viable based upon the Check Point Security Gateway data retrieved. The verification process checks that:

- the Operating System and currently distributed packages are appropriate for the package to be distributed,
- there is sufficient disk space,
- the package is not already distributed,
- the package dependencies are fulfilled.

To manually verify a distribution, select **Packages > Pre-Install Verifier**.

Transferring Files to Remote Devices

When you are ready to upgrade or distribute packages from the **Package Repository**, it is recommended to transfer the package files to the devices to be upgraded. Placing the file on the remote device shortens the overall installation time, frees Security Management server for other operations, and reduces the chance of a communications error during the distribute/upgrade process. Once the package file is located on the remote device, you can activate the distribute/upgrade whenever it is convenient.

Transfer the package file(s) to the directory $SUROOT/tmp on the remote device. If this directory does not exist, do one of the following:

- For Windows gateways, place the package file in the directory SYSTEMDRIVE\temp (SYSTEMDRIVE is usually C:\)
- For UNIX gateways, place the package file in the directory /opt/.

Performing Distributions and Upgrades

There are two methods for performing distributions (that is, installations) and upgrades. In one operation you can upgrade all packages on a single remote gateway, or you can distribute specific packages one-by-one.

Upgrading All Packages on a Check Point Remote Gateway

All Check Point packages on a single remote gateway, other than the operating system, can be remotely upgraded in a single operation. The **Upgrade all Packages** function allows you to simultaneously distribute or upgrade multiple packages to the latest management version. Proceed as follows:

1. Select **Packages > Upgrade all Packages**.
2. From the **Upgrade All Packages** window, select the Check Point Security Gateways that you want to upgrade. Use the **Ctrl** and **Shift** keys to select multiple devices.

   **Note** - The **Reboot if required...** option (checked by default) is required in order to activate the newly distributed package.

3. If one or more of the required packages are missing from the **Package Repository**, the **Download Packages** window opens. Download the required package directly to the **Package Repository**.
4. Click **Upgrade**.

   The installation proceeds only if the upgrade packages for the selected packages are available in the **Package Repository**.

Updating a Single Package on a Check Point Remote Gateway

Use this procedure to select the specific package that you want to apply to a single package. The **distribute** function allows you to:

- Upgrade the OS on an IP appliance or on SecurePlatform
- Upgrade any package to a management version other than the latest
- Apply Hot Fix Accumulators (HFAs)

Proceed as follows:

1. In the **Package Management** window, click the Check Point Security Gateway you want to upgrade.
2. Select **Packages > distribute**.
3. From the **distribute Packages** window, select the package that you want to distribute. Use the Ctrl and Shift keys to select multiple packages, and then click **distribute**.

The installation proceeds only if the upgrade packages selected are available in the **Package Repository**.

**Upgrading UTM-1 Edge Firmware with SmartUpdate**

The UTM-1 Edge gateway firmware represents the software that is running on the appliance. The UTM-1 Edge gateway’s firmware can be viewed and upgraded using SmartUpdate. This is a centralized management tool that is used to upgrade all gateways in the system by downloading new versions from the download center. When installing new firmware, the firmware is prepared at the Security Management server, downloaded and subsequently installed when the UTM-1 Edge gateway fetches for updates. Since the UTM-1 Edge gateway fetches at periodic intervals, you will notice the upgraded version on the gateway only after the periodic interval has passed.

If you do not want to wait for the fetch to occur you can download the updates with the **Push Packages Now (UTM-1 Edge only)** option in the **Packages** menu. With this option it is possible to create a connection with UTM-1 Edge in order to access new (that is, the latest) software package(s). The distribution is immediate and avoids the need to wait for the fetch to get the package.

**Other Upgrade Operations**

**Canceling an Operation**

You can halt the distribution (that is, installation) or upgrade while in progress. To cancel an operation:

- Select **Status > Stop Operation**.

At a certain point in any operation, the **Stop Operation** function becomes unavailable. If you decide you want to cancel after this point is reached, wait for the operation to complete, and then select **Packages > Uninstall**.

**Uninstalling Distributions and Upgrades**

If you want to cancel an operation and you have passed the point of no return, or the operation has finished, you can uninstall the upgrade by selecting **Packages > Uninstall**.

*Note* - Uninstallation restores the gateway to the last management version distributed.

**Rebooting the Check Point Security Gateway**

After distribution (that is, installation) or uninstallation, it is recommended to reboot the gateway.

To reboot the gateway, either:

- Check the **Reboot if required**... property during the final stage of each respective operation, or
- Select **Packages > Reboot Gateway**.

**Recovering From a Failed Upgrade**

If an upgrade fails on SecurePlatform, SmartUpdate restores the previously distributed version.

**SecurePlatform Automatic Revert**

If an upgrade or distribution operation fails on a SecurePlatform device, the device will reboot itself and automatically revert to the last version distributed.
Snapshot Image Management

Before performing an upgrade, you can use the command line to create a Snapshot image of the SecurePlatform OS, or of the packages distributed. If the upgrade or distribution operation fails, you can use the command line to revert the disk to the saved image.

- To create a Snapshot file on the gateway, type:
  
  `cprinstall snapshot <object name> <filename>`

- To show the available Snapshot files, type:
  
  `cprinstall show <object name>`

- To revert to a given Snapshot file, type:
  
  `cprinstall revert <object name> <filename>`

  **Note**: Snapshot files are stored at `/var/CPsnapshot` on the gateway.

Deleting Packages From the Package Repository

To clear the Package Repository of extraneous or outdated packages, select a package, or Ctrl-select multiple packages and select Packages > Delete Package. This operation cannot be undone.

Managing Licenses

Overview of Managing Licenses

With SmartUpdate, you can manage all licenses for Check Point packages throughout the organization from the Security Management server. SmartUpdate provides a global view of all available and installed licenses, allowing you to perform such operations as adding new licenses, attaching licenses and upgrading licenses to Check Point Security Gateways, and deleting expired licenses. Check Point licenses come in two forms, Central and Local.

- The **Central** license is the preferred method of licensing. A Central license ties the package license to the IP address of the Security Management server. That means that there is one IP address for all licenses; that the license remains valid if you change the IP address of the gateway; and that a license can be taken from one Check Point Security Gateway and given to another with ease. For maximum flexibility, it is recommended to use Central licenses.

- The **Local** license is an older method of licensing, however it is still supported by SmartUpdate. A Local license ties the package license to the IP address of the specific Check Point Security Gateway, and cannot be transferred to a gateway with a different IP address.

When you add a license to the system using SmartUpdate, it is stored in the License & Contract Repository. Once there, it must be installed to the gateway and registered with the Security Management server. Installing and registering a license is accomplished through an operation known as **attaching** a license. Central licenses require an administrator to designate a gateway for attachment, while Local licenses are automatically attached to their respective Check Point Security Gateways.

Licensing Terminology

- **Add**
  Licenses received from the User Center should first be added to the License & Contract Repository. Adding a local license to the License & Contract Repository also attaches it to the gateway.
  Licenses can be conveniently imported to the License & Contract Repository via a file and they can be added manually by pasting or typing the license details.

- **Attach**
Licenses are attached to a gateway via SmartUpdate. Attaching a license to a gateway involves installing the license on the remote gateway, and associating the license with the specific gateway in the License & Contract Repository.

- **Central License**
  A Central License is a license attached to the Security Management server IP address, rather than the gateway IP address. The benefits of a Central License are:
  - Only one IP address is needed for all licenses.
  - A license can be taken from one gateway and given to another.
  - The new license remains valid when changing the gateway IP address. There is no need to create and install a new license.

- **Certificate Key**
  The Certificate Key is a string of 12 alphanumeric characters. The number is unique to each package. For an evaluation license your certificate key can be found inside the mini pack. For a permanent license you should receive your certificate key from your reseller.

- **CPLIC**
  A command line for managing local licenses and local license operations. For additional information, refer to the R71 Command Line Interface Reference Guide.

- **Detach**
  Detaching a license from a gateway involves uninstalling the license from the remote gateway and making the license in the License & Contract Repository available to any gateway.

- **State**
  Licenses can be in one of the following states:
  The license state depends on whether the license is associated with the gateway in the License & Contract Repository, and whether the license is installed on the remote gateway. The license state definitions are as follows:
  - **Attached** indicates that the license is associated with the gateway in the License & Contract Repository, and is installed on the remote gateway.
  - **Unattached** indicates that the license is not associated with the gateway in the License & Contract Repository, and is not installed on any gateway.
  - **Assigned** is a license that is associated with the gateway in the License & Contract Repository, but has not yet been installed on a gateway.

- **Upgrade Status** is a field in the License & Contract Repository that contains an error message from the User Center when the Upgrade process fails.

- **Get**
  Locally installed licenses can be placed in the License & Contract Repository, in order to update the repository with all licenses across the installation. The Get operation is a two-way process that places all locally installed licenses in the License & Contract Repository and removes all locally deleted licenses from the License & Contract Repository.

- **License Expiration**
  Licenses expire on a particular date, or never. After a license has expired, the functionality of the Check Point package may be impaired.

- **Local License**
  A Local License is tied to the IP address of the specific gateway and can only be used with a gateway or a Security Management server with the same address.

- **Multi-License File**
  Licenses can be conveniently added to a gateway or a Security Management server via a file, rather than by typing long text strings. Multi-license files contain more than one license, and can be downloaded from the User Center (http://usercenter.checkpoint.com).
  Multi-license files are supported by the cplic put, and cplic add command-line commands.

- **Features**
  A character string that identifies the features of a package.
License Upgrade

One of the many SmartUpdate features is to upgrade licenses that reside in the License & Contract Repository. SmartUpdate will take all licenses in the License & Contract Repository, and will attempt to upgrade them with the use of the Upgrade tool.

For a full explanation on how to upgrade licenses, refer to *R71 Installation and Upgrade Guide*.

The License Attachment Process

**Introducing the License Attachment Process**

When a Central license is placed in the License & Contract Repository, SmartUpdate allows you to attach it to Check Point packages. Attaching a license installs it to the remote gateway and registers it with the Security Management server.

New licenses need to be attached when:

- An existing license expires.
- An existing license is upgraded to a newer license.
- A Local license is replaced with a Central license.
- The IP address of the Security Management server or Check Point Security Gateway changes.

Attaching a license is a three step process.

1. Get real-time license data from the remote gateway.
2. Add the appropriate license to the License & Contract Repository.
3. Attach the license to the device.

The following explains the process in detail.

**Retrieving License Data From Check Point Security Gateways**

To know exactly what type of license is on each remote gateway, you can retrieve that data directly from the gateway.

- To retrieve license data from a single remote gateway, right-click on the gateway in the License Management window and select Get Check Point Security Gateway Licenses.
- To retrieve license data from multiple Check Point Security Gateways, from the Licenses menu and select Get All Licenses.

**Adding New Licenses to the License & Contract Repository**

To install a license, you must first add it to the License & Contract Repository. You can add licenses to the License & Contract Repository in the following ways:

**Download From the User Center**

1. Select Licenses & Contracts > Add License > From User Center
2. Enter your credentials.
3. Perform one of the following:
   - Generate a new license - if there are no identical licenses, the license is added to the License & Contract Repository.
   - Change the IP address of an existing license, that is, Move IP.
   - Change the license from Local to Central.

**Importing License Files**

2. Browse to the location of the license file, select it, and click Open.
A license file can contain multiple licenses. Unattached Central licenses appear in the License & Contract Repository, and Local licenses are automatically attached to their Check Point Security Gateway. All licenses are assigned a default name in the format SKU@ time date, which you can modify at a later time.

Add License Details Manually

You may add licenses that you have received from the Licensing Center by email. The email contains the license installation instructions.

1. Locate the license:
   - If you have received a license by email, copy the license to the clipboard. Copy the string that starts with cplic putlic... and ends with the last SKU/Feature. For example: cplic putlic 1.1.1.1 06Dec2002 dw59Ufa2-eLLQ9NB-gPuyHzvQ-WKreSo4Zx CPSUITE-EVAL-3DES-NGX CK-1234567890
   - If you have a hard copy printout, continue to step 2.

2. Select the License & Contracts tab in SmartUpdate.


4. Enter the license details:
   - If you copied the license to the clipboard, click Paste License. The fields will be populated with the license details.
   - Alternatively, enter the license details from a hard-copy printout.

5. Click Calculate, and make sure the result matches the validation code received from the User Center.

6. You may assign a name to the license, if desired. If you leave the Name field empty, the license is assigned a name in the format SKU@ time date.

7. Click OK to complete the operation.

Attaching Licenses

After licenses have been added to the License & Contract Repository, select one or more licenses to attach to a Check Point Security Gateway.

1. Select the license(s).
2. Select Licenses & Contracts > Attach.
3. From the Attach Licenses window, select the desired device.

If the attach operation fails, the Local licenses are deleted from the Repository.

Other License Operations

Detaching Licenses

Detaching a license involves deleting a single Central license from a remote Check Point Security Gateway and marking it as unattached in the License & Contract Repository. This license is then available to be used by any Check Point Security Gateway.

To detach a license, select Licenses & Contracts > Detach and select the licenses to be detached from the displayed window.

Note - Local licenses, prior to NGX R62, cannot be detached from a remote Check Point Security Gateway.

Deleting Licenses From the License & Contract Repository

Licenses that are not attached to any Check Point Security Gateway and are no longer needed can be deleted from the License & Contract Repository.
To delete a license:
1. Right-click anywhere in the License & Contract Repository and select View Unattached Licenses.
2. Select the unattached license(s) to be deleted, and click Delete.

Viewing License Properties

The overall view of the License & Contract Repository displays general information on each license such as the name of the license and the IP address of the machine to which it is attached. You can view other properties as well, such as expiration date, SKU, license type, certificate key and signature key.

To view license properties, double-click on the license in the Licenses tab.

Checking for Expired Licenses

After a license has expired, the functionality of the Check Point package will be impaired; therefore, it is advisable to be aware of the pending expiration dates of all licenses.

To check for expired licenses, select Licenses > Show Expired Licenses.

To check for licenses nearing their dates of expiration:
1. In the License Expiration window, set the Search for licenses expiring within the next \(x\) days property.
2. Click Apply to run the search.

To delete expired licenses from the License Expiration window, select the detached license(s) and click Delete.

Exporting a License to a File

Licenses can be exported to a file. The file can later be imported to the License & Contract Repository. This can be useful for administrative or support purposes.

To export a license to a file:
1. In the Licenses Repository, select one or more licenses, right-click, and from the menu select Export to File....
2. In the Choose File to Export License(s) To window, name the file (or select an existing file), and browse to the desired location. Click Save.

All selected licenses are exported. If the file already exists, the new licenses are added to the file.

Service Contracts

Before upgrading a gateway or Security Management server, you need to have a valid support contract that includes software upgrade and major releases registered to your Check Point User Center account. The contract file is stored on Security Management server and downloaded to Check Point Security Gateways during the upgrade process. By verifying your status with the User Center, the contract file enables you to easily remain compliant with current Check Point licensing standards.

For more information on service contracts, see the R71 Installation and Upgrade Guide or visit Service Contract Files Web page (http://www.checkpoint.com/ngx/upgrade/contract/index.html).

Generating CPInfo

CPInfo is a support tool that gathers into one text file a wide range of data concerning the Check Point packages in your system. When speaking with a Check Point Technical Support Engineer, you may be asked to run CPInfo and transmit the data to the Support Center.

To launch CPInfo, select Tools > Generate CPInfo.
1. Choose the directory to which you want to save the output file.
2. Choose between two methods to name the file:
   - based on the SR number the technician assigns you, or
   - a custom name that you define.

3. Optionally, you may choose to add:
   - **log files** to the CPInfo output.
   - the **registry** to the CPInfo output.

---

**The SmartUpdate Command Line**

All management operations that are performed via the SmartUpdate GUI can also be executed via the command line. There are three main commands:

- **cppkg** to work with the Packages Repository.
- **cprinstall** to perform remote installations of packages.
- **cplic** for license management.

For details on how to use these commands, see the *R71 Command Line Interface Reference Guide* (http://supportcontent.checkpoint.com/documentation_download?id=10324).
Chapter 10

SmartDirectory (LDAP) and User Management

This chapter assumes that you have working knowledge of LDAP technology.

In This Chapter

- Integrating LDAP Servers with Check Point Software
- The Check Point Solution for Using LDAP Servers
- SmartDirectory (LDAP) Considerations
- Configuring SmartDirectory (LDAP) Entities
- SmartDirectory (LDAP) Reference Information

Integrating LDAP Servers with Check Point Software

When Check Point software is purchased, you may already have an effective user management infrastructure, such as LDAP. The Security Management server supports LDAP technology and uses existing LDAP servers to obtain user information for authentication and authorization purposes.

If you do not have a user management infrastructure in place, you can make a choice between managing customers on the internal users database or choosing to implement an LDAP server. If you have a large user count, it is recommended to opt for an external user management database, such as LDAP. By maintaining the large user database externally, the Security Management server performance is greatly enhanced. For example, if the user database is external, the database will not have to be reinstalled every time the user information changes. Additionally, the LDAP user database can be used as the user database by other applications.

The Check Point Solution for Using LDAP Servers

Check Point products are compliant with LDAP technology. This compliancy enables:

- Users to be managed externally by an LDAP server.
- The gateways to retrieve CRLs.
- User information from other applications gathered in the LDAP users database to be shared by many different applications. The Security Management server uses the user information for authentication purposes.

LDAP is an open industry standard that is used by multiple vendors. It is widely accepted as the directory access method of the Internet. One of the reasons that it is the obvious choice for so many vendors is because of its cross-platform compliancy. LDAP is automatically installed on different Operating Systems (e.g. the Microsoft Active Directory) and servers (such as Novell, Netscape etc.).

When integrated with the Security Management server, LDAP is referred to as SmartDirectory (LDAP).
SmartDirectory (LDAP) Deployment

When deployed with a SmartDirectory (LDAP) server, the Security Management server and the Security Gateways function as SmartDirectory (LDAP) clients. As shown in the diagram:

- The Security Management server manages the user information on the SmartDirectory (LDAP) server
- The gateways acts as a SmartDirectory (LDAP) client in order to:
  - Query user information
  - Retrieve CRLs
  - In some cases, perform bind operations for authentication purposes.

There are several SmartDirectory (LDAP) features that can be applied to further enhance SmartDirectory (LDAP) functionality, these include:

- **High Availability**, where user information can be duplicated across several servers (SmartDirectory [LDAP] Replications). See Account Units and High Availability (on page 117).
- Support of *multiple SmartDirectory (LDAP) servers* on which many user databases are distributed. See Working with Multiple SmartDirectory (LDAP) Servers (on page 119).
- **The use of encrypted or non-encrypted SmartDirectory (LDAP) Connections**. The administrator must decide, for each SmartDirectory (LDAP) server specified in the Account Unit, whether the SmartDirectory (LDAP) connections are encrypted between the SmartDirectory (LDAP) server and the Security Management server or Security Gateways using SSL, or whether they are "clear", that is, not encrypted. See Define an Account Unit (see "Define an LDAP Account Unit" on page 121).
- **Support of Multiple SmartDirectory (LDAP) Vendors by using Profiles**. Built in profiles are available for different supported platforms. These profiles can be selected and applied to an Account Unit. This enables the system to adapt to the specified SmartDirectory (LDAP) server and to recognize from which vendor it originated. To this end, all SmartDirectory (LDAP) servers specified on an Account Unit must be of the same vendor. When the Security Management server queries a given SmartDirectory (LDAP) server, the queries will be customized according to the selected profile. The default profiles can be modified. See SmartDirectory (LDAP) Profiles (on page 120).

Account Units

An *Account Unit* is the interface which allows interaction between the Security Management server and Security Gateways, and the SmartDirectory (LDAP) server(s).

Each Account Unit represents one or more branches of the information maintained on the SmartDirectory (LDAP) server. An organization may have several Account Units, which represent the various SmartDirectory (LDAP) servers. In this case, the users in the system are split between the different Account...
Units, as well as between the different branches within the Account Unit. For instance, in a bank with one SmartDirectory (LDAP) server, one Account Unit may represent users with businesses accounts and another Account Unit may represent users with private accounts. Within the former, large business users may be defined in one branch and small business users may be defined on another branch.

In order to work with SmartDirectory (LDAP) servers, the administrator needs to:

- define the Account Unit(s) that represents the organization
- enter the access information required in order to connect to the relevant SmartDirectory (LDAP) server.

After this is done, the Security Management server or Security Gateways can then connect to that SmartDirectory (LDAP) server in order to manage the users or to make queries.

### The SmartDirectory (LDAP) Schema

The SmartDirectory (LDAP) server has a default schema which is simply a description of the structure of the data in a SmartDirectory (LDAP) directory. It includes user definitions defined for that proprietary SmartDirectory (LDAP) server. This schema does not possess Security Management server and Security Gateway specific information, such as IKE-related attributes, authentication schemes and values for remote users.

It is possible to make do with the default SmartDirectory (LDAP) schema. Especially in the case when all users use the same authentication scheme and are defined according to a default template. However, if the users in the database have different definitions, it is more effective to apply a Check Point schema to the SmartDirectory (LDAP) server. The Check Point schema complements the structure of the information in the SmartDirectory (LDAP) server and provides Security Management server and Security Gateway specific information. See Check Point Schema (on page 119).

### Account Units and High Availability

If you are using SmartDirectory (LDAP) replications for High Availability purposes, the same Account Unit can be used to represent all the replicated SmartDirectory (LDAP) servers. For example, two SmartDirectory (LDAP) server replications can be defined on the same Account Unit, and two different Check Point gateways can each use the same Account unit.
When SmartDirectory (LDAP) servers are queried for user information, they are queried according to their place in a set priority. Priority is defined on two levels: per gateway as well as per Account Unit. When per gateway, the priority of the SmartDirectory (LDAP) servers is defined according to their proximity. The closest SmartDirectory (LDAP) server has the first priority. The furthest SmartDirectory (LDAP) server has the last priority. In the event that a specified gateway does not have a set SmartDirectory (LDAP) server priority, the Account Unit has a default SmartDirectory (LDAP) server priority list. SmartDirectory (LDAP) servers with the same priority are queried in a round-robin manner for load-balancing purposes.

If you have SmartDirectory (LDAP) server replications and you are using the Security Management server to manage users, you need to select the SmartDirectory (LDAP) server to which the Security Management server connects. The Security Management server can work with one SmartDirectory (LDAP) server. All other replications must be properly synchronized with the SmartDirectory (LDAP) server.

Managing Users on a SmartDirectory (LDAP) Server

In order to manage users on a SmartDirectory (LDAP) server a special license is required. Once the license has been obtained, an Account Unit that represents the SmartDirectory (LDAP) server needs to be defined. The users and user groups are arranged on the Account Unit in a tree structure which reflects the structure of the SmartDirectory (LDAP) server. This tree reflects the internal user hierarchy of the organization represented by the Account Unit. Users that are managed on an external SmartDirectory (LDAP) server are managed (added, edited or deleted) as if they were users managed by the Security Management server.

There are two main difference between user management on the internal database, and user management on a SmartDirectory (LDAP) server. Firstly, user management in the SmartDirectory (LDAP) server is done externally and not locally. Secondly, on a SmartDirectory (LDAP) server templates can be modified and applied to users dynamically. This means that user definitions are easy to change and to manage; and changes are instantaneous or “live”. Changes that are applied to a SmartDirectory (LDAP) template are reflected immediately for all users who are using that template.
Retrieving Information from a SmartDirectory (LDAP) Server

When a gateway requires user information for authentication purposes, it searches for this information in three different places:

1. The first place that is queried is the internal users database.
2. If the specified user is not defined in this database, the gateway queries the SmartDirectory (LDAP) servers defined in the Account Unit one at a time, and according to their priority. If for some reason the query against a specified SmartDirectory (LDAP) server fails, for instance the SmartDirectory (LDAP) connection is lost, the SmartDirectory (LDAP) server with the next highest priority is queried. If there is more than one Account Unit, the Account Units are queried concurrently. The results of the query are either taken from the first Account Unit to meet the conditions, or from all the Account Units which meet the conditions. The choice between taking the result of one Account Unit as opposed to many is a matter of gateway configuration.
3. If the information still cannot be found, the gateway uses the external users template to see if there is a match against the generic profile. This generic profile has the default attributes applied to the specified user.

For performance issues, it is better to query SmartDirectory (LDAP) Account Units when there are open connections. For this reason, some open connections are maintained by the gateways. These open connections will be used in order to execute a series of queries on user information, such as:

- Who is the user?
- To what groups does the user belong?

A SmartDirectory (LDAP) group is a user group which consists of members who are defined on a SmartDirectory (LDAP) server and not on the internal Security Management server database. For more information, see SmartDirectory (LDAP) Groups (on page 125).

The gateway queries the SmartDirectory (LDAP) server in order to determine if the user belongs to a group that is permitted to perform certain operations, (for instance whether the user is allowed to open a VPN tunnel).

Working with Multiple SmartDirectory (LDAP) Servers

Distributing Users across Multiple SmartDirectory (LDAP) Servers

The users of an organization may be distributed across several SmartDirectory (LDAP) servers. Each SmartDirectory (LDAP) server must be represented by a separate Account Unit.

Querying Multiple SmartDirectory (LDAP) Servers

The Security Management server and the gateways can work with multiple SmartDirectory (LDAP) servers concurrently. For example, if a gateway needs to find user information, and it does not know where the specified user is defined, it is able to query all the SmartDirectory (LDAP) servers in the system. (Sometimes a gateway may be able to ascertain the location of a user by looking at the user DN when working with certificates).

Check Point Schema

The SmartDirectory (LDAP) schema is the default schema which assigns objects their properties and attributes. While it is often enough to work with the default, in certain cases, like when the default authentication scheme and the default templates are not used globally by all users, it is advisable to enhance the default SmartDirectory (LDAP) schema by adding the Check Point schema.

The Check Point schema acts as an extension to the default SmartDirectory (LDAP) schema. It can be used in order to enhance the definition of various objects for extended user authentication functionality. For example, an Object Class entitled fw1Person is part of the Check Point schema. This Object Class has some mandatory and some optional attributes and it enhances the definition of the Person attribute. Another example is fw1Template. This is a standalone attribute which is used to define a template of user
information to which a user can be associated. See SmartDirectory (LDAP) Schema (see “The SmartDirectory (LDAP) Schema” on page 117) for the Check Point schema.

SmartDirectory (LDAP) Profiles

There are different LDAP servers which are designed by several different LDAP vendors. SmartDirectory (LDAP) profiles are assigned to ensure that the default attributes for a given SmartDirectory (LDAP) server are properly in place. In other words, if you have a certified OPSEC SmartDirectory (LDAP) server, apply the OPSEC_DS profile to get enhanced OPSEC-specific SmartDirectory (LDAP) server attributes.

The existing SmartDirectory (LDAP) servers and SmartDirectory (LDAP) deployments differ in terms of object repositories, schema, and object relations. The following examples illustrate this variety:

- The organization's user database may have unconventional object types and relations due to the use of a specific application.
- Some applications use the cn attribute in the User object's Relatively Distinguished Name (RDN) while others use uid.
- In Microsoft Active Directory, the user attribute memberOf describes which group the user belongs to, while standard LDAP schemes define the member attribute in the group object itself.
- Different servers implement different storage formats for passwords.
- Some servers are considered v3 but do not implement some of v3 specifications. Therefore, the organizations using such servers will not be able to extend the schema.
- Some LDAP servers already have built in support for certain user data while others require a Check Point schema extended attribute. For example, Microsoft Active Directory has the accountExpires user attribute while other SmartDirectory (LDAP) servers require the Check Point attribute fw1expirationdate which is part of the Check Point defined fw1person objectclass.
- Some servers allow queries with non-defined types while others do not.

To help the administrators successfully cope with diverse technical solutions, a new layer, SmartDirectory (LDAP) profiles, has been added that controls most of the SmartDirectory (LDAP) server-specific knowledge. The SmartDirectory (LDAP) profile is a configurable LDAP policy that allows administrators to define more precise SmartDirectory (LDAP) requests and enhance communication with the server.

Modifying SmartDirectory (LDAP) Profiles

Profiles consist of three major categories

- **Common** - this category lists profile settings that are common both when reading and writing to the SmartDirectory (LDAP) server
- **Read** - this category lists profile settings that are relevant only when reading from the SmartDirectory (LDAP) server
- **Write** - this category lists profile settings that are relevant only when writing to the SmartDirectory (LDAP) server

Some of these categories list the same entry with different values. This is because the behavior differs depending on the type of operation.

Default SmartDirectory (LDAP) Profiles

Four profiles are defined by default, each corresponding to a specific SmartDirectory (LDAP) server:

- **OPSEC_DS** - the default profile for a standard OPSEC certified SmartDirectory (LDAP) server
- **Netscape_DS** - the profile for a Netscape Directory Server
- **Novell_DS** - the profile for a Novell Directory Server
- **Microsoft_AD** - the profile for Microsoft Active Directory.
Working with the SmartDirectory (LDAP) Profile

The profile is selected and applied during the creation or modification of a SmartDirectory (LDAP) Account Unit. However, you can modify certain parameters of the default profiles for finer granularity and performance tuning. This is done by copying the settings of an existing SmartDirectory (LDAP) profile into a newly created profile and then modifying the profile to fit the requirements.

See Modifying SmartDirectory (LDAP) Profiles (on page 120) for details on how to modify SmartDirectory (LDAP) profiles.

SmartDirectory (LDAP) Considerations

The key to effective use of SmartDirectory (LDAP) servers is careful planning. The system administrator needs to decide:

- How to use the SmartDirectory (LDAP) server, whether for user management, CR retrieval, user authentication or all three.
- How many SmartDirectory (LDAP) servers to use. If High Availability is being implemented, the use of Replications also needs to be carefully considered.
  For each SmartDirectory (LDAP) server an Account Unit needs to be created to represent it. Account Units need to be properly installed in a place whether they can communicate securely and effectively with the gateways.
- The priority (for High Availability and querying purposes) of the SmartDirectory (LDAP) servers. The order of priority of SmartDirectory (LDAP) servers is defined in two places: on the Account Unit and on the gateway. The priority for the SmartDirectory (LDAP) server may be different on these entities. Generally, the priority for gateways is defined according to proximity, where the nearest SmartDirectory (LDAP) server has the highest priority.
- Users need to be effectively and efficiently spread out across the available Account Units, branches and sub branches. Moreover, they need to be classified in logical groups whose members all share a common thread (such as role in the organization, permissions, etc.).

Configuring SmartDirectory (LDAP) Entities

The predominant reasons for integrating the Security Management server and Security Gateways with SmartDirectory (LDAP) are:

- To query user information
- To enable User management
- To enable CRL retrieval
- To authenticate users

The first step for any of these objectives is to define an Account Unit. If you are implementing SmartDirectory (LDAP) user management, you will need to know which entities to define, and how to manage the users defined on the SmartDirectory (LDAP) server. SmartDirectory (LDAP) user management requires a special license.

Define an LDAP Account Unit

To define an LDAP account unit:

1. In the Objects Tree > Servers tab, right-click Servers and select New > LDAP Account Unit.
The LDAP Account Unit Properties window opens.

**Figure 10-16** LDAP Account Unit Properties Window

2. Enter a name for the SmartDirectory (LDAP) Account Unit.

3. Decide whether this Account Unit is to be used for Certificate Revocation List (CRL retrieval), **User Management** or both.

   **Note** - Single Sign On for LDAP users will only work if **user management** is selected.

4. Select a profile to be applied to the new Account Unit.

5. In the **Servers** tab, select the SmartDirectory (LDAP) servers to be used by the Account Unit.

   The order in which they are displayed is also the default order in which they will be queried. This priority can be defined per gateway or on the Account Unit.

6. In the **Objects Management** tab, select the SmartDirectory (LDAP) server on which the objects are managed.

   Branches of the server will be searched when this SmartDirectory (LDAP) server is queried.

   To retrieve the branches, click **Fetch branches**. If it is disabled (some versions of SmartDirectory (LDAP) do not support automatic branch retrieval), define the branches manually:

   a) Click **Add**.

   b) In the **LDAP Branch Definition window**, enter the **Branch Path**.

   For enhanced security, this Account Unit object can be locked with a password which must be entered when this Account Unit is accessed from SmartDashboard for managing users.

7. In the **Authentication** tab, define the authentication limitations and default authentication settings for a user on an Account Unit. The Allowed Authentication schemes limit the user's authentication access only to those authentication schemes. You can allow several authentication schemes which can be applied per user, or you can apply a default scheme which is applied to all the users.

   Users that are retrieved through this Account Unit, but which are missing authentication-related definitions, will be granted these definitions using the default authentication scheme, or a complete user template.

   These default settings are useful if the Check Point schema is not in place. In place of the Check Point schema, a user template is used to supply the authentication attributes. The other options described on this page will be automatically configured per user.

   For all users in this Account Unit that are configured for IKE, the pre-shared secret for encryption purposes should be entered.
The number of login attempts to a user can be set, as well as the number of seconds it takes for the user's account to be unlocked, once it has been frozen.

To modify the LDAP servers in an LDAP Account Unit:

Double-click a server in the LDAP Account Unit Properties > Servers tab. The LDAP Server Properties window is displayed.

**Figure 10-17** SmartDirectory (LDAP) Server Properties window

- In the General tab:
  - Change the server port.
  - Modify the login DN of the server.
  - Specify a password to be used for authentication purposes.
  - Define the priority of the selected server within the account unit.
  - Define gateway access permissions for this server.

- In the Encryption tab:
  - Define whether SmartDirectory (LDAP) connections are SSL encrypted.
  - If the connections are encrypted, define the relevant encryption port and the minimum and maximum encryption strengths.
  - Verify the Fingerprints by comparing the displayed fingerprint with the SmartDirectory (LDAP) Fingerprint.

**Note** - SmartDirectory (LDAP) connections can be authenticated by using client certificates that are supplied by a trust Certificate Authority (CA) ("Authenticating with the SmartDirectory (LDAP) Server using Certificates" on page 126). To use certificates, the SmartDirectory (LDAP) server must be configured with SSL strong authentication.

**Working with SmartDirectory (LDAP) for User Management**

1. Once a proper license has been obtained, enable SmartDirectory (LDAP) SmartDirectory and configure the SmartDirectory (LDAP) attributes in the SmartDirectory (LDAP) SmartDirectory page of the Global Properties window. Access this window by selecting Policy > Global Properties.
2. Define the Check Point host on which the SmartDirectory (LDAP) server resides (see the following figure).

**Figure 10-18** Defining a new SmartDirectory (LDAP) server in the Objects Tree

3. Define a SmartDirectory (LDAP) Account Unit in the **SmartDirectory (LDAP) Account Unit Properties** window (see the following figure). Specify that the Account Unit is to be used for user management.

**Figure 10-19** Defining a new SmartDirectory (LDAP) Account Unit in the Objects Tree

**Working with SmartDirectory (LDAP) for CRL Retrieval**

1. Define the Check Point host on which the SmartDirectory (LDAP) server resides (see the following figure).

**Figure 10-20** Defining a new SmartDirectory (LDAP) server in the Objects Tree

2. Define a SmartDirectory (LDAP) Account Unit in the **SmartDirectory (LDAP) Account Unit Properties** window (see the following figure). Specify that the Account Unit is to be used CRL retrieval.

**Figure 10-21** Defining a new SmartDirectory (LDAP) Account Unit in the Objects Tree

**Managing Users**

Users that are defined on the Account Unit are managed in the **Users** tab of the Objects Tree.
This intuitive tree structure enables users to be managed as if they were actually sitting on the internal Security Management server database. For instance, you can add, edit or delete users by right-clicking on them in the Objects Tree, and by selecting the option of your choice.

**Figure 10-22 Creating a new SmartDirectory (LDAP) User**

![Image of SmartDirectory (LDAP) user management](image)

**SmartDirectory (LDAP) Groups**

SmartDirectory (LDAP) groups are created in order to classify users within certain group types. These SmartDirectory (LDAP) groups are thereafter applied in Policy rules. Define a SmartDirectory (LDAP) group in the **SmartDirectory Group Properties** window in the **Users and Administrators** tab of the Objects tree.

Once SmartDirectory (LDAP) groups are created, they can be applied in various policy rules, such as the Security Policy, etc.

In this window, you can select the Account Unit on which the SmartDirectory (LDAP) group is defined. Apply an advanced filter in order to increase the granularity of a group definition. Only those users who match the defined criteria will be included as members of the SmartDirectory (LDAP) group. For instance, you can include all users defined on the selected Account Unit as part of the SmartDirectory (LDAP) group, or only members of a specified branch, or only members of a specified group on the branch.

For advanced treatment of the SmartDirectory (LDAP) group, a filter can be applied which allows for the use of additional SmartDirectory (LDAP) criteria. Only the users who match these criteria will be applied as group members.

**How are SmartDirectory (LDAP) users grouped?**

SmartDirectory (LDAP) users can be grouped logically: for instance, all SmartDirectory (LDAP) users from the same Account Unit, or from the same sub-branch of the Account Unit can be grouped together, or SmartDirectory (LDAP) users that share membership to the same SmartDirectory (LDAP) group object can be grouped together.

SmartDirectory (LDAP) users can be grouped dynamically according to a dynamic filter.

**Examples**

- If the User objects for managers in your enterprise include the additional object class "myOrgManager", you can define the Managers group by specifying the additional filter (objectclass=myOrgManagers).
• If certain users in your enterprise have an e-mail address ending with us.org.com, you can define the US group by specifying the additional filter (mail=*us.org.com).

Figure 10-23 Defining a new SmartDirectory (LDAP) Group in the Objects Tree

Authenticating with the SmartDirectory (LDAP) Server using Certificates

The Security Management server and its gateways can be issued special certificates in order to allow them to communicate with SmartDirectory (LDAP) server. The proper Encryption attributes need to be set in the SmartDirectory (LDAP) Server Properties window, and in addition, the following procedure needs to take place:

1. Use the dbedit command to manually set a flag in the objects_5_0.C file for every desired SmartDirectory (LDAP) server, as well as Replications. Set the ldap_use_cert_auth attribute to true for every entry in the fields attribute of the Account Unit.

2. Log on to SmartDashboard and add a Certificate Authority (CA) object for the CA that will issue the certificate for each Check Point object that uses SmartDirectory (LDAP) certificate based authentication. For more information, see the PKI chapter in the R71 Virtual Private Networks Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10320).

3. Add a certificate for all necessary network objects (such as VPN, Policy Server, or firewall) that require certificate-based SmartDirectory (LDAP) connections. In the VPN page, add a certificate issued by the CA defined above. For more information, see the PKI chapter in the R71 Virtual Private Networks Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10320).

4. In the Users and Administrators tab of the Objects tree, check the new configuration by opening a connection on one of the Account Units configured to use certificate authentication.

Using SmartDirectory (LDAP) Queries

Queries can be used to determine SmartDirectory (LDAP) user or group information. The SmartDirectory (LDAP) servers that are specified in the Account Unit can be configured to allow themselves to be queried.

To query SmartDirectory (LDAP) Users and Groups, right-click the SmartDirectory (LDAP) Account Unit in the Users tab of the Objects tree, and select Query Users/Group. The SmartDirectory (LDAP) Query Search window is displayed.

Figure 10-24 Making a SmartDirectory (LDAP) query

This window can be used for simple as well as advanced queries.
Defining Queries

1. Select an attribute, an operator and a value for each query. These represent the component being queried, the condition of the query and the specific item.

   For example, \(<\text{mail}, \text{contains}, \text{Andy},\text{>}\) means that all \textit{mail} that \textit{contains} the value \textit{Andy} should be found. The operators are explained in the following table.

   \begin{table}
   \centering
   \caption{Operators - meaning of values}
   \begin{tabular}{|l|l|}
   \hline
   \textbf{Value} & \textbf{Meaning} \\
   \hline
   \textit{is} & The attribute's value must be equal to the Value. \\
   \textit{is not} & The attribute's value is not equal to the Value. \\
   \textit{starts with} & The attribute's value starts with the Value. \\
   \textit{ends with} & The attribute's value ends with the Value. \\
   \textit{contains} & The attribute's value contains the Value. \\
   \textit{equal or less than} & The attribute's value is less than or equal to the Value. \\
   \textit{equal or greater than} & The attribute's value is greater than or equal to the Value. \\
   \textit{sounds like} & The attribute's value sounds like the Value. \\
   \hline
   \end{tabular}
   \end{table}

   \textbf{Note} - The "less than" and "greater than" operators are supported by LDAP Version 3.0 and higher servers only.

2. There are several advanced methods which can be applied to enhance your queries. Click \textbf{Advanced} to see these options, which include:
   - click \textit{Add} each time you would like to filter by another criterion, after selecting the new attributes, operators and values.
   - enter a free form SmartDirectory (LDAP) expression. See RFC 1558 for information about the syntax of SmartDirectory (LDAP) query expressions
   - use the Boolean AND/OR conditions
   - object types can selected in order to narrow the query. For instance, you can filter by users, groups and templates.

3. Click \textbf{Find} to run the query.

When a query is executed, the SmartDirectory (LDAP) server queries the SmartDirectory (LDAP) directory, using a filter constructed from the query. For example, the previous query becomes the following filter:

\[
\text{filter:} (\&(\{|\text{objectclass=fw1person}\} \& \{|\text{objectclass=person}\} \& \{|\text{objectclass=organizationalPerson}\} \& \{|\text{objectclass/inetOrgPerson}\}) \& (\{|\text{cn=Brad}\} \& \{|\text{mail=*Andy*}\})))
\]
Integration with Various SmartDirectory (LDAP) Vendors

**Microsoft Active Directory**

The Microsoft Windows 2000 advanced server (or later) includes a sophisticated SmartDirectory (LDAP) server that can be adjusted to work as a user database for the Security Management server.

By default, the Active Directory services are disabled. In order to enable the directory services:

- run the `dcpromo` command from the **Start > Run** menu, or
- run the Active Directory setup wizard using the **System Configuration** window.

The Active Directory has the following structure:

```
DC=qa, DC=checkpoint,DC=com
CN=Configuration,DCROOT
CN=Schema,CN=Configuration,DCROOT
CN=System,DCROOT
CN=Users,DCROOT
CN=Builtin,DCROOT
CN=Computers,DCROOT
OU=Domain Controllers,DCROOT
...
```

Most of the user objects and group objects created by Windows 2000 tools are stored under the `CN=Users, DCROOT` branch, others under `CN=Builtin, DCROOT` branch, but these objects can be created under other branches as well.

The branch `CN=Schema, CN=Configuration, DCROOT` contains all schema definitions.

Check Point can take advantage of an existing Active Directory object as well as add new types. For users, the existing user can be used "as is" or be extended with `fw1person` as an auxiliary of "User" for full feature granularity. The existing Active Directory "Group" type is supported "as is". A SmartDirectory (LDAP) template can be created by adding the `fw1template` objectclass. This information is downloaded to the directory using the `schema_microsoft_ad.ldif` file (see Adding New Attributes to the Active Directory (on page 129)).

**Performance**

The number of queries performed on the directory server is significantly low with Active Directory. This is achieved by having a different object relations model. The Active Directory group-related information is stored inside the user object. Therefore, when fetching the user object no additional query is necessary to assign the user with the group. The same is true for users and templates.

**Manageability**

SmartDashboard allows the creation and management of existing and new objects. However, some specific Active Directory fields are not enabled via SmartDashboard.

**Enforcement**

It is possible to work with the existing Active Directory objects without extending the schema. This is made possible by defining an Internal Template object and assigning it with the SmartDirectory (LDAP) Account Unit defined on the Active Directory server.
For example, if you wish to enable all users with IKE+Hybrid based on the Active Directory passwords, create a new template with the IKE properties enabled and "Check Point password" as the authentication method.

**Modifying the Active Directory Schema**

**Updating the registry settings**

To modify the Active Directory schema, add a new registry DWORD key named `Schema Update Allowed` with the value different from zero under `HKLM\System\CurrentControlSet\Services\NTDS\Parameters`.

**Delegating Control**

Delegating control over the directory to a specific user or group is important since by default the Administrator is not allowed to modify the schema or even manage directory objects through SmartDirectory (LDAP) protocol.

To delegate control over the directory:
1. Display the Users and Computers Control console.
2. Right-click on the domain name displayed in the left pane and choose Delegate control from the right-click menu.
   - The Delegation of Control wizard window is displayed.
3. Add an Administrator or another user from the System Administrators group to the list of users who can control the directory.
4. Reboot the machine.

**Adding New Attributes to the Active Directory**

Below is the example in LDAP Data Interchange (LDIF) format that adds one attribute to the Microsoft Active Directory:

```plaintext
dn: CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
changeType: add
adminDisplayName: fw1auth-method
attributeID: 1.3.114.7.4.2.0.1
attributeSyntax: 2.5.5.4
cn: fw1auth-method
distinguishedName:
CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
instanceType: 4
isSingleValued: FALSE
LDAPDisplayName: fw1auth-method
name: fw1auth-method
objectCategory:
CN=Attribute-Schema,CN=Configuration,CN=Schema,
CN=Configuration,DCROOT
ObjectClass: attributeSchema
oMSyntax: 20
rangeLower: 1
rangeUpper: 256
```
All Check Point attributes can be added in a similar way. The definitions of all attributes in LDIF format are contained in the `schema_microsoft_ad.ldif` file located in the `$FWDIR/lib/ldap` directory.

Before attempting to run the `ldapmodify` command, edit `schema_microsoft_ad.ldif` and replace all instances of `DCROOT` with the specific domain root of your organization. For example if your domain is `support.checkpoint.com`, replace `DCROOT` with `dc=support,dc=checkpoint,dc=com`.

After modifying the file, run the `ldapmodify` command to load the file into the directory. For example if you use the Administrator account of the `dc=support,dc=checkpoint,dc=com` domain the command syntax will be as follows:

```
ldapmodify -c -h support.checkpoint.com -D cn=administrator,cn=users,dc=support,dc=checkpoint,dc=com" -w SeCrEt -f
$FWDIR/lib/ldap/schema_microsoft_ad.ldif
```

**Note** - A shell script is available for UNIX gateways. The script is located at: `$FWDIR/lib/ldap/update_schema_microsoft_ad`.

**Netscape LDAP Schema**

If you would like to add the propriety schema to your Netscape directory server, use the file `schema.ldif` which is located in the `$FWDIR/lib/ldap` directory.

How is the Netscape Schema Updated?

You should use the file `update_schema.ldif` which is located in the `$FWDIR/lib/ldap` directory.

The ldif file performs the following operations:

- adds the new attributes to the schema
- deletes old definitions of `fw1person` and `fw1template`
- adds new definitions of `fw1person` and `fw1template`. 
Important - This operation deletes the objectclass definition from the schema and adds the updated one instead. It is recommended to backup the SmartDirectory (LDAP) server before this operation. You can use this file with the `ldapmodify` command line. On some server versions the delete objectclass operation may return with error although it was successful. You can run `ldapmodify` with `-c` (continuous) option.

SmartDirectory (LDAP) Schema

Schema Checking

When schema checking is enabled, SmartDirectory (LDAP) requires that every object class and its associated attributes be defined in the directory schema.

Before working with SmartDirectory (LDAP), schema checking should be disabled. Once the Check Point object classes and attributes to the SmartDirectory (LDAP) server's schema, schema checking should be enabled.

Proprietary Attributes

OID

Each of the proprietary object classes and attributes (all of which begin with "fw1") has a proprietary Object Identifier (OID), listed below.

Table 10-9 Object Class OIDs

<table>
<thead>
<tr>
<th>object class</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw1template</td>
<td>1.3.114.7.4.2.0.1</td>
</tr>
<tr>
<td>fw1person</td>
<td>1.3.114.7.4.2.0.2</td>
</tr>
</tbody>
</table>

The OIDs for the proprietary attributes begin with the same prefix ("1.3.114.7.4.2.0.X"). Only the value of "X" is different for each attribute. See Attributes (on page 131) for the value of "X".

Attributes

The following attributes are available:

- cn (on page 132)
- uid (on page 133)
- description (on page 133)
- mail (on page 133)
- member (on page 133)
- userPassword (on page 133)
- fw1authmethod (on page 133)
- fw1authserver (on page 134)
The entry's name. This is also referred to as "Common Name". For users this can be different from the uid attribute, the name used to login to the Security Gateway. This attribute is also used to build the SmartDirectory (LDAP) entry's distinguished name, that is, it is the RDN of the DN.
uid

The user's login name, that is, the name used to login to the Security Gateway. This attribute is passed to the external authentication system in all authentication methods except for "Internal Password", and must be defined for all these authentication schemes.

The login name is used by the Security Management server to search the SmartDirectory (LDAP) server(s). For this reason, each user entry should have its own unique uid value.

It is also possible to login to the Security Gateway using the full DN. The DN can be used when there is an ambiguity with this attribute or in "Internal Password" when this attribute may be missing. The DN can also be used when the same user (with the same uid) is defined in more than one Account Unit on different SmartDirectory (LDAP) servers.

description

Descriptive text about the user.

    default
    "no value"

mail

User's email address.

    default
    "no value"

member

An entry can have zero or more values for this attribute.

- In a template: The DN of user entries using this template. DNs that are not users (object classes that are not one of: "person", "organizationalPerson", "inetOrgPerson" or "fw1person") are ignored.

- In a group: The DN of user.

userPassword

Must be given if the authentication method (fw1auth-method) is "Internal Password". The value can be hashed using "crypt". In this case the syntax of this attribute is:

"{crypt}xxyyyyyyyyyy"

where "xx" is the "salt" and "yyyyyyyyyy" is the hashed password.

It is possible (but not recommended) to store the password without hashing. However, if hashing is specified in the SmartDirectory (LDAP) server, you should not specify hashing here, in order to prevent the password from being hashed twice. You should also use SSL in this case, to prevent sending an unencrypted password.

The Security Gateway never reads this attribute, though it does write it. Instead, the SmartDirectory (LDAP) bind operation is used to verify a password.

fw1authmethod

One of the following:

RADIUS, TACACS, SecurID, OS Password, Defender

This default value for this attribute is overridden by Default Scheme in the Authentication tab of the Account Unit window in SmartDashboard. For example: a SmartDirectory (LDAP) server can contain SmartDirectory (LDAP) entries that are all of the object-class "person" even though the proprietary object-class "fw1person" was not added to the server's schema. If Default Scheme in SmartDashboard is
"Internal Password", all the users will be authenticated using the password stored in the "userPassword" attribute.

**fw1authserver**

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>y</td>
<td>y</td>
<td>&quot;undefined&quot;</td>
</tr>
</tbody>
</table>

The name of the server that will perform the authentication. This field must be given if fw1auth-method is "RADIUS" or "TACACS". For all other values of fw1auth-method, it is ignored. Its meaning is given below:

<table>
<thead>
<tr>
<th>method</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>name of a RADIUS server, a group of RADIUS servers, or &quot;Any&quot;</td>
</tr>
<tr>
<td>TACACS</td>
<td>name of a TACACS server</td>
</tr>
</tbody>
</table>

**fw1pwdLastMod**

The date on which the password was last modified. The format is `yyyymmdd` (for example, 20 August 1998 is 19980820). A password can be modified through the Security Gateway as a part of the authentication process.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>y</td>
<td>y</td>
<td>If no value is given, then the password has never been modified.</td>
</tr>
</tbody>
</table>

**fw1expiration-date**

The last date on which the user can login to a Security Gateway, or "no value" if there is no expiration date. The format is `yyyymmdd` (for example, 20 August 1998 is 19980820). The default is "no value".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>y</td>
<td>y</td>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

**fw1hour-range-from**

The time from which the user can login to a Security Gateway. The format is `hh:mm` (for example, 8:15 AM is 08:15).
fw1hour-range-to
The time until which the user can login to a Security Gateway. The format is $hh:mm$ (for example, 8:15 AM is 08:15).

<table>
<thead>
<tr>
<th>“X” in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>y</td>
<td>y</td>
<td>“00:00”</td>
</tr>
</tbody>
</table>

fw1day
The days on which the user can login to a Security Gateway. Can have the values "SUN","MON",…etc.

<table>
<thead>
<tr>
<th>“X” in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>y</td>
<td>y</td>
<td>all days of the week</td>
</tr>
</tbody>
</table>

fw1allowed-src
The names of one or more network objects from which the user can run a client, or "Any" to remove this limitation, or "no value" if there is no such client. The names should match the name of network objects defined in Security Management server.

<table>
<thead>
<tr>
<th>“X” in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>y</td>
<td>y</td>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

fw1allowed-dst
The names of one or more network objects which the user can access, or "Any" to remove this limitation, or "no value" if there is no such network object. The names should match the name of network objects defined on the Security Management server.

<table>
<thead>
<tr>
<th>“X” in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>y</td>
<td>y</td>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

fw1allowed-vlan
Not currently used.

<table>
<thead>
<tr>
<th>“X” in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>y</td>
<td>y</td>
<td>&quot;no value&quot;</td>
</tr>
</tbody>
</table>

fw1SR-keym
The algorithm used to encrypt the session key in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".

<table>
<thead>
<tr>
<th>“X” in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>y</td>
<td>y</td>
<td>&quot;Any&quot;</td>
</tr>
</tbody>
</table>
fw1SR-datam

The algorithm used to encrypt the data in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>y</td>
<td>y</td>
<td>&quot;Any&quot;</td>
</tr>
</tbody>
</table>

fw1SR-mdm

The algorithm used to sign the data in SecuRemote. Can be "none" or "MD5".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>y</td>
<td>y</td>
<td>&quot;none&quot;</td>
</tr>
</tbody>
</table>

fw1enc-fwz-expiration

The number of minutes after which a SecuRemote user must re-authenticate himself or herself to the Security Gateway.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>y</td>
<td>y</td>
</tr>
</tbody>
</table>

fw1sr-auth-track

The exception to generate on successful authentication via SecuRemote. Can be "none", "cryptlog" or "cryptalert".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>y</td>
<td>y</td>
<td>&quot;none&quot;</td>
</tr>
</tbody>
</table>

fw1groupTemplate

This flag is used to resolve a problem related to group membership.

The group membership of a user is stored in the group entries to which it belongs, in the user entry itself, or in both entries. Therefore there is no clear indication in the user entry if information from the template about group relationship should be used.

If this flag is "TRUE", then the user is taken to be a member of all the groups to which the template is a member. This is in addition to all the groups in which the user is directly a member.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>y</td>
<td>y</td>
<td>&quot;False&quot;</td>
</tr>
</tbody>
</table>

fw1ISAKMP-EncMethod

The key encryption methods for SecuRemote users using IKE. This can be one or more of: "DES", "3DES". A user using IKE (formerly known as ISAMP) may have both methods defined.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>y</td>
<td>y</td>
<td>&quot;DES&quot;, &quot;3DES&quot;</td>
</tr>
</tbody>
</table>
fw1ISAKMP-AuthMethods
The allowed authentication methods for SecuRemote users using IKE, (formerly known as ISAMP). This can be one or more of: "preshared", "signatures".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>y</td>
<td>y</td>
<td>&quot;signatures&quot;</td>
</tr>
</tbody>
</table>

fw1ISAKMP-HashMethods
The data integrity method for SecuRemote users using IKE, (formerly known as ISAMP). This can be one or more of: "MD5", "SHA1". A user using IKE must have both methods defined.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>y</td>
<td>y</td>
<td>&quot;MD5&quot;, &quot;SHA1&quot;</td>
</tr>
</tbody>
</table>

fw1ISAKMP-Transform
The IPSec Transform method for SecuRemote users using IKE, (formerly known as ISAMP). This can be one of: "AH", "ESP".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>y</td>
<td>y</td>
<td>&quot;ESP&quot;</td>
</tr>
</tbody>
</table>

fw1ISAKMP-DataIntegrityMethod
The data integrity method for SecuRemote users using IKE, (formerly known as ISAMP). This can be one of: "MD5", "SHA1".

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>y</td>
<td>y</td>
<td>&quot;SHA1&quot;</td>
</tr>
</tbody>
</table>

fw1ISAKMP-SharedSecret
The pre-shared secret for SecuRemote users using IKE, (formerly known as ISAMP).
The value can be calculated using the fw ikecrypt command line.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>y</td>
<td>y</td>
</tr>
</tbody>
</table>

fw1ISAKMP-DataEncMethod
The data encryption method for SecuRemote users using IKE, (formerly known as ISAMP).

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>y</td>
<td>y</td>
<td>&quot;DES&quot;</td>
</tr>
</tbody>
</table>
fw1enc-Methods

The encryption method allowed for SecuRemote users. This can be one or more of: "FWZ", "ISAKMP" (meaning IKE).

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
<th>fw1template</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>y</td>
<td>y</td>
<td>&quot;FWZ&quot;</td>
</tr>
</tbody>
</table>

fw1userPwdPolicy

Defines when and by whom the password should and can be changed.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>y</td>
</tr>
</tbody>
</table>

fw1badPwdCount

Number of allowed wrong passwords entered sequentially.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>y</td>
</tr>
</tbody>
</table>

fw1lastLoginFailure

Time of the last login failure.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>4</td>
</tr>
</tbody>
</table>

memberof template

DN of the template that the user is a member of.

<table>
<thead>
<tr>
<th>&quot;X&quot; in OID</th>
<th>fw1person</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>4</td>
</tr>
</tbody>
</table>

Modifying SmartDirectory (LDAP) Profiles

The `objects.c` file contains four profiles, each corresponding to a SmartDirectory (LDAP) server type.

Profile Attributes

The attributes that are commonly configured by category are described.

UserLoginAttr

The unique username SmartDirectory (LDAP) attribute (uid). In addition, when fetching users by the username, this attribute is used for query.
UserPasswordAttr

This user password SmartDirectory (LDAP) attribute.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>uid (most servers)</td>
</tr>
<tr>
<td></td>
<td>SamAccountName (in Microsoft_AD)</td>
</tr>
<tr>
<td></td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

TemplateObjectClass

The object class for Check Point SmartDirectory (LDAP) templates. If you change the default value with another objectclass, make sure to extend that objectclass schema definition with relevant attributes from fw1template.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>fw1template</td>
</tr>
<tr>
<td></td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

ExpirationDateAttr

The account expiration date SmartDirectory (LDAP) attribute. This could be a Check Point extended attribute or an existing attribute.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw1expiration-date</td>
<td>One value allowed</td>
</tr>
<tr>
<td>accountExpires</td>
<td></td>
</tr>
<tr>
<td>(in Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>

ExpirationDateFormat

Expiration date format. This format will be applied to the value defined at ExpirationDateAttr.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CP format is yyyyymmdd</td>
</tr>
<tr>
<td></td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

PsswdDateformat

The format of the password modified date SmartDirectory (LDAP) attribute. This formation will be applied to the value defined at PsswdDateAttr.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP (most servers)</td>
<td>One value allowed</td>
</tr>
<tr>
<td>format is yyyyymmdd</td>
<td></td>
</tr>
<tr>
<td>MS (in Microsoft_AD)</td>
<td></td>
</tr>
</tbody>
</table>
**PsswdDateAttr**

The password last modified date SmartDirectory (LDAP) attribute.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>fw1pwdLastMod (most servers)</td>
</tr>
<tr>
<td></td>
<td>pwdLastSet (in Microsoft_AD)</td>
</tr>
</tbody>
</table>

**BadPwdCountAttr**

SmartDirectory (LDAP) attribute to store and read bad password authentication count.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw1BadPwdCount</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**ClientSideCrypt**

If 0, the sent password will not be encrypted. If 1, the sent password will be encrypted with the algorithm specified in the DefaultCryptAlgorithm.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1 for Netscape_DS</td>
</tr>
<tr>
<td></td>
<td>if not using encrypted password, SSL is recommended</td>
</tr>
</tbody>
</table>

**DefaultCryptAlgorithm**

The algorithm used to encrypt a password before updating the SmartDirectory (LDAP) server with a new password.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain (for most servers)</td>
<td>One value allowed</td>
</tr>
<tr>
<td>Crypt (for Netscape_DS)</td>
<td>One value allowed</td>
</tr>
<tr>
<td>SHA1</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**CryptedPasswordPrefix**

The text to prefix to the encrypted password when updating the SmartDirectory (LDAP) server with a modified password.

<table>
<thead>
<tr>
<th>default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>{Crypt} (for Netscape_DS)</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**PhoneNumberAttr**

SmartDirectory (LDAP) attribute to store and read the user phone number.
AttributesTranslationMap

General purpose attribute translation map, to resolve problems related to peculiarities of different server types. For example, an X.500 server does not allow the "-" character in an attribute name. To enable the Check Point attributes containing "-", specify a translation entry: (e.g., "$fw1-expiration =fw1expiration").

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Other</td>
</tr>
<tr>
<td>internationalisednumber</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

ListOfAttrsToAvoid

All attribute names listed here will be removed from the default list of attributes included in read/write operations. This is most useful in cases where these attributes are not supported by the SmartDirectory (LDAP) server schema, which might fail the entire operation. This is especially relevant when the SmartDirectory (LDAP) server schema is not extended with the Check Point schema extension.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are no values by default. In case the SmartDirectory (LDAP) server was not extended by the Check Point schema, the best thing to do is to list here all the new Check Point schema attributes.</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

BranchObjectClass

Use this attribute to define which type of objects (objectclass) is queried when the object tree branches are displayed after the Account Unit is opened in SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Organization OrganizationalUnit Domain (most servers)</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td>• Container (extra for Microsoft_AD)</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

BranchOCOperator

If One is set, an ORed query will be sent and every object that matches the criteria will be displayed as a branch. If All, an ANDed query will be sent and only objects of all types will be displayed.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

OrganizationObjectClass

This attribute defines what objects should be displayed with an organization object icon. A new object type specified here should also be in BranchObjectClass.
### OrgUnitObjectClass
This attribute defines what objects should be displayed with an organization object icon. A new object type specified here should also be in BranchObjectClass.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>organization</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

- organizationalUnit (most servers)
- Contained (added to Microsoft_AD)

### DomainObjectClass
This attribute defines what objects should be displayed with a Domain object icon. A new object type specified here should also be in BranchObjectClass.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

### UserObjectClass
This attribute defines what objects should be read as user objects. The user icon will be displayed on the tree for object types specified here.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>User (in Microsoft_AD)</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td>Person</td>
<td></td>
</tr>
<tr>
<td>OrganizationalPerson</td>
<td></td>
</tr>
<tr>
<td>InertOrgPerson</td>
<td></td>
</tr>
<tr>
<td>FW1 Person (most servers)</td>
<td></td>
</tr>
</tbody>
</table>

### UserOCOperator
If 'one' is set, an ORed query will be sent and every object that matches one of the types will be displayed as a user. If 'all' and ANDed query will be sent and only objects of all types will be displayed.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

### GroupObjectClass
This attribute defines what objects should be read as groups. The group icon will be displayed on the tree for objects of types specified here.
<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groupofnames</td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td></td>
<td>Group of uniquenames (most servers)</td>
</tr>
<tr>
<td></td>
<td>Group</td>
</tr>
<tr>
<td></td>
<td>Group of names (in Microsoft_AD)</td>
</tr>
</tbody>
</table>

**GroupOCOperator**

If 'one' is set an ORed query will be sent and every object that matches one of the types will be displayed as a user. If 'all' an ANDed query will be sent and only objects of all types will be displayed.

**GroupMembership**

Defines the relationship mode between the group and its members (user or template objects) when reading group membership.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
</table>
| One     | One value allowed

- Member mode defines the member DN in the Group object (most servers)
- MemberOf mode defines the group DN in the member object (in Microsoft_AD)
- Both mode defines both the member DN in the Group object and the group DN in the Member object.

**UserMembershipAttr**

Defines what SmartDirectory (LDAP) attribute to use when reading group membership from the user or template object if GroupMembership mode is 'MemberOf' or 'Both' you may be required to extend the user/template object schema in order to use this attribute.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
</table>
| MemberOf | One value allowed

**TemplateMembership**

Defines the user to template membership mode when reading user template membership information.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

- Member mode defines the member DN in the Group object (most servers)
- MemberOf mode defines the group DN in the member object (in Microsoft_AD)

**TemplateMembershipAttr**

Defines which attribute to use when reading the User members from the template object, as User DNs, if the TemplateMembership mode is Member.
Default | Other
--- | ---
member | Multiple values allowed

**UserTemplateMembershipAttr**

 Defines which attribute to use when reading from the User object the template DN associated with the user, if the TemplateMembership mode is MemberOf.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>member</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**OrganizationRDN**

 This value will be used as the attribute name in the Relatively Distinguished Name (RDN) when creating a new organization via SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>o</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**OrgUnitRDN**

 This value will be used as the attribute name in the Relatively Distinguished Name (RDN) when creating a new organizationalUnit via SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>ou</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**UserRDN**

 This value will be used as the attribute name in the Relatively Distinguished Name (RDN) when creating a new User object via SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**GroupRDN**

 This value will be used as the attribute name for the RDN when creating a new Group object via SmartDashboard.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**DomainRDN**

 This value will be used as the attribute name for the RDN when creating a new Domain object via SmartDashboard.
**AutomaticAttrs**

This field is relevant when creating objects in SmartDashboard. The format of this field is `Objectclass:name:value` meaning that if the object being created is of type `ObjectClass` then additional attributes will be included in the created object with name `name` and value `value`.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dc</code></td>
<td>One value allowed</td>
</tr>
</tbody>
</table>

**GroupObjectClass**

This field is used when modifying an existing group in SmartDashboard. The format of this field is `ObjectClass:memberattr` meaning that for each group objectclass there is a group membership attribute mapping. List here all the possible mappings for this SmartDirectory (LDAP) server profile. When a group is modified, based on the group’s objectclass the right group membership mapping will be used.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>groupOfNames:member</code></td>
<td>Multiple values allowed</td>
</tr>
<tr>
<td><code>groupOfUniqueNames:uniqueMember</code></td>
<td></td>
</tr>
<tr>
<td>(All other servers)</td>
<td></td>
</tr>
</tbody>
</table>

**OrgUnitObjectClass**

This determines which ObjectClass to use when creating/modifying an OrganizationalUnit object. These values can be different from the read counterpart.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>OrganizationalUnit</code></td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**OrganizationObjectClass**

This determines which ObjectClass to use when creating and/or modifying an Organization object. These values can be different from the read counterpart.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Organization</code></td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**UserObjectClass**

This determines which ObjectClass to use when creating and/or modifying a user object. These values can be different from the read counterpart.
**Default** | **Other**
---|---
User (in Microsoft_AD) user organizationalPerson inetOrgPerson fw1Person (All other servers) | Multiple values allowed

**DomainObjectClass**

Determines which ObjectClass to use when creating and/or modifying a domain context object. These values can be different from the read counterpart.

<table>
<thead>
<tr>
<th>Default</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Multiple values allowed</td>
</tr>
</tbody>
</table>

**Fetch User Information Effectively by Modifying the Profile**

SmartDirectory (LDAP) servers organize groups and members through different means and relations. SmartDirectory (LDAP) operations are performed by Check Point on users, groups of users, and user templates where the template is defined as a group entry and users are its members. The mode in which groups/templates and users are defined has a profound effect on the performance of some of the Check Point functionality when fetching user information. There are three different modes:

- Defining a "Member" attribute per member, or "Member" user-to-group membership mode. In this case, each member of a specific group gets the "Member" attribute, where the value of this attribute is the DN of that member.
- Defining a "Memberof" attribute per group, or "Memberof" user-to-group membership mode. In this case, each group gets the "Memberof" attribute per group, where the value of this attribute is the DN of a group entry. This is referred to as "Memberof" user-to-group membership mode.
- Defining a "Memberof" attribute per member and group, or "Both" user-to-group membership mode. In this case both members and groups are given the "Memberof" attribute.

The most effective mode is the "Memberof" and "Both" modes where user's groups membership information is available on the user itself and no additional SmartDirectory (LDAP) queries are necessary.

**Setting the User-to-Group Membership Mode**

Set the user-to-group membership mode in the profile objects for each SmartDirectory (LDAP) server in objects_5_0.C.

- To specify the user-to-group and template-to-group membership mode set the `GroupMembership` attribute to one of the following values: Member, MemberOf, Both accordingly.
- To specify the user-to-template membership mode set the `TemplateMembership` attribute to one of the following values: Member, MemberOf accordingly.

After successfully converting the database, set the SmartDirectory (LDAP) server profile in objects_5_0.C to the proper membership setting and start the Security Management server. Make sure to install policy/user database on all gateways to enable the new configuration.
Chapter 11

Management High Availability

In This Chapter

The Need for Management High Availability 147
The Management High Availability Solution 147
Management High Availability Considerations 151
Management High Availability Configuration 152

The Need for Management High Availability

The Security Management server consists of several databases with information on different aspects of the system, such as objects, users and policy information. This data changes each time the system administrator makes modifications to the system. It is important to maintain a backup for this data, so that crucial information is not permanently lost in the event of Security Management server failure.

Moreover, if the Security Management server fails or is down for administrative purposes, a backup server needs to be in place in order to take over its activities. In the absence of the Security Management server, essential operations performed by the gateways, such as the fetching of the Security Policy and the retrieval of the CRL, cannot take place.

The Management High Availability Solution

Backing Up the Security Management server

In Management High Availability, the Active Security Management server (Active SMS) always has one or more backup Standby Security Management servers (Standby SMS) which are ready to take over from the Active Security Management server. These Security Management servers must all be of the same Operating System and version. The existence of the Standby SMS allows for crucial backups to be in place:

- for the Security Management server - the various databases in the corporate organization, such as the database of objects and users, policy information and ICA files are stored on both the Standby SMSs as well as the Active SMS. These Security Management servers are synchronized so data is maintained and ready to be used. If the Active SMS is down a Standby SMS needs to become Active in order to be able to edit and install the Security Policy.

- for the Security Gateway - certain operations that are performed by the Security Gateways via the Active SMS, such as fetching a Security Policy, or retrieving a CRL from the Security Management server, can be performed on Standby SMS.
In a Management High Availability deployment, the first installed Security Management server is specified as the Primary Security Management server. This is a regular Security Management server used by the system administrator to manage the Security Policy. When any subsequent Security Management server is installed, these must be specified as Secondary Security Management servers. Once the Secondary Security Management server has been installed and manually synchronized, the distinctions between Primary versus Secondary are no longer significant. These servers are now referred to according to their role in the Management High Availability scenario as Active or Standby, where any Security Management server can function as the Active SMS.

The Management High Availability Environment

The Management High Availability environment requires an Active SMS and at least one Standby SMS. The Secondary SMS is created with empty databases. These databases are filled with information that the newly created Secondary SMS gleans from the Active SMS. The Secondary SMS is ready once:

- it is represented on the Primary Security Management server by a network object
- SIC has been initialized between it and the Primary Security Management server
- manual synchronization has been done with the Primary Security Management server for the first time.

It is possible to install a gateway on any of the Security Management servers. The role of these gateways is to protect the Security Management servers. Although the Security Management servers backup one another, High Availability is not implemented between the gateways installed on Security Management servers.

Active versus Standby

All management operations such as editing and installing the Security Policy and modifying users and objects, are done by the Active SMS. If the Active SMS is down, and any of the aforementioned operations need to be performed, one of the Standby SMSs should be made active by the system administrator. This transition from Standby to Active should be initiated manually.

The Standby SMSs are synchronized to the Active SMS, and therefore, are kept up to date with all changes in the databases and Security Policy. Thus Security Gateways can fetch the Security Policy and retrieve a CRL from both the Active SMS and the Standby SMS.

The frequency of the synchronization between the Standby SMS and the Active SMS is set by the System Administrator. This process can be configured to take place automatically, or it can be set to occur manually.
What Data is Backed Up by the Standby Security Management servers?

In order for Management High Availability to function properly, the following data must be synchronized and backed up:

- configuration and ICA data, such as:
  - databases (such as the Objects and Users).
  - certificate information such as Certificate Authority data and the CRL which is available to be fetched by the Check Point Security Gateways.
- the latest installed Security Policy. The installed Security Policy is the applied Security Policy. The Security Gateways must be able to fetch the latest Security Policy from either the Active or the Standby SMS.

**Note** - Previous versions of the Database, SmartMap data, as well as View Installed Policy data are not synchronized.

Synchronization Modes

There are two ways to perform synchronization:

- **manual synchronization** is a process initialized by the system administrator. It can be set to synchronize either databases, or databases as well as the installed Security Policy.
  
  The former option synchronizes quicker than the latter option. It should be the preferred mode of synchronization provided that the system administrator has edited the objects or the Security Policy, but has not installed the newly edited Security Policy since the previous synchronization.

- **automatic synchronization** is a process configured by the system administrator to allow the Standby SMSs to be synchronized with the Active SMSs at set intervals of time. This is generally the preferred mode of synchronization, since it keeps the Standby SMSs updated. The basis for the synchronization schedule is that when the Security Policy is installed, both the installed Security Policy and all the databases are synchronized. Additionally, it is possible to synchronize the Standby SMSs when:
  - the system administrator saves the Security Policy
  - at a specified scheduled time

Even when automatic synchronization has been selected as the synchronization mode, it is possible to perform a manual synchronization.

Synchronization Status

The synchronization status indicates the status of the peer SMSs in relation to that of the selected Security Management server. This status can be viewed in the Management High Availability Servers window or in SmartView Monitor, whether you are connected to the Active or Standby SMS.

**Figure 11-26** A typical Management High Availability scenario

The possible synchronization statuses are:
• *Never been synchronized* - immediately after the Secondary Security Management server has been installed, it has not yet undergone the first manual synchronization that brings it up to date with the Primary Security Management server.

• *Synchronized* - the peer is properly synchronized and has the same database information and installed Security Policy.

• *Lagging* - the peer SMS has not been synchronized properly.
  
  For instance, on account of the fact that the Active SMS has undergone changes since the previous synchronization (objects have been edited, or the Security Policy has been newly installed), the information on the Standby SMS is lagging.

• *Advanced* - the peer SMS is more up-to-date.
  
  For instance, in the above figure, if a system administrators logs into Security Management server B before it has been synchronized with the Security Management server A, the status of the Security Management server A is Advanced, since it contains more up-to-date information which the former does not have.

  In this case, manual synchronization must be initiated by the system administrator by changing the Active SMS to a Standby SMS. Perform a *synch me* operation from the more advanced server to the Standby SMS. Change the Standby SMS to the Active SMS.

• *Collision* - the Active SMS and its peer have different installed policies and databases. The administrator must perform manual synchronization and decide which of the SMSs to overwrite.

  For instance, in the above figure, when Security Management server A fails before a synchronization takes place, the changes made (to databases or to the Security Policy) cannot be synchronized with Security Management server B. When Security Management server B takes over from Security Management server A, the system administrator may decide to modify the Security Policy.

  In this case, both Security Management server A and B have some information which is not synchronized with its peer. In order to remedy the collision state, one of the Security Management servers will need to be overwritten. The Security Management server which is found to have the dominant or significant changes should be the Security Management server on which manual synchronization is initiated.

  At this point the system administrator needs to decide which of the Security Management server’s should become the Standby SMS, and change its status, if necessary.

**Note** - Changes made by the CA, such as the issuance of certificates, could lead to breaches of security if they are overwritten; therefore, any CA changes that are made are merged in order to eliminate security issues.

### Changing the Status of the Security Management server

Although Security Gateways can use the Standby Security Management server to fetch a Security Policy or a fresh CRL, in the event that the Active SMS fails, the Standby SMS must become the Active SMS for two predominant reasons:

1. The Standby SMS cannot perform management operations such as editing and installing the Security Policy. While the Standby is identical in its databases and installed Security Policy to the Active SMS, if changes are needed for the Security Policy the Standby SMS does not have the capacity to make them.

2. The ICA database can only be modified on the Active SMS.

If the Active SMS is going down for administrative purposes, the system administrator should login to the Standby SMS and manually set it as the Active SMS.

Thereafter manual synchronization should be initiated. Once the Standby SMS has become the Active SMS, it is recommended to perform an Install Policy operation, in order to verify that this machine is functioning properly as an Active SMS.

If the Active SMS is in failover, it is likely that the synchronization status of the Active SMS and its peer will be collision. In this case the system administrator will need to decide which information will be overwritten.
Synchronization Diagnostics

The status of all Security Management servers can be viewed in the Management High Availability Servers window in SmartDashboard or via SmartView Monitor. Audit Logs can be used to view and track management operations as well as Synchronization operations in the SmartView Tracker.

When Synchronization Fails

There are several instances in which the synchronization process might fail:

- synchronization failure - for instance, the Active SMS was unable to make a connection with the Standby SMS at the moment of synchronization. To solve this:
  - manually synchronize the Standby SMS at a later opportunity, or
  - if you are working in automatic mode, reinstall the Security Policy when the Standby SMS can be reached. After the install operation takes place, synchronization occurs automatically.

- Collision between the Security Management servers. In this case the system administrator should perform a manual synchronization and decide which database is the dominant database. The CA is always merged in order to eliminate security issues.

When a collision occurs and one of the Security Management servers is overwritten, it is very useful to follow management operations performed on the overwritten Security Management server in the audit logs of the SmartView Tracker. In this manner it is possible to track and redo these operations, where necessary, on the dominant Security Management server.

Management High Availability Considerations

Remote versus Local Installation of the Secondary SMS

In the Management High Availability deployment the Secondary SMS is often installed locally on the LAN. The system administrator should consider the usefulness of maintaining a remote Standby SMS. This remote Security Management server will not be affected in the case of networking problems on the LAN. This Standby SMS can be made into the Active SMS by the remote system administrator.

Different Methods of Synchronization

Automatic synchronization keeps the peer SMSs updated. However the synchronization may take some time and affect the system performance. It may be useful to schedule a synchronization event that automatically synchronizes the Security Management servers after working hours when the system performance cannot affect the regular work of the employees.

Manual synchronization can be initiated at any stage by the system administrator. Manual synchronization is recommended when changing the Standby SMS to Active (if the Active SMS is about to go down for administrative purposes). It is essential when the synchronization status is collision.

Data Overload During Synchronization

The data saved during the synchronization process is very heavy. Synchronization is optimized if the connectivity between the Security Management server is fast and efficient.
Management High Availability Configuration

Secondary Management Creation and Synchronization - the First Time

1. When installing the Security Management server in a Management High Availability deployment you will be prompted to specify whether it is the Primary Management or the Secondary Management. Select the latter.

2. In SmartDashboard, create a network object to represent the Secondary Security Management server, as follows:
   a) Select Manage > Network Objects > Check Point > New > Host.

   ![Figure 11-27](image)

   Figure 11-27 Initializing the Secondary Management

   In the displayed window:

   b) In the Software Blades, section, select the Management tab, and select Secondary Server. This automatically selects the Logging and Status as well.

   Note - In order for the Secondary Security Management server to act as a Log Server when the Primary Security Management server becomes unavailable, additional steps must be performed. Access the Security Gateway properties window, and select Logs and Masters > Log Servers. Add the Secondary Security Management server to the When a Log Server is unreachable, send logs to list.
c) Initialize SIC between the Secondary Security Management server and the Active SMS by selecting Communication.


Changing the Active SMS to the Standby SMS

1. On the Active SMS, display the Management High Availability Server window by selecting Policy > Management High Availability.
2. In the displayed window, click Change to Standby.

Figure 11-28 Check Point Security Management and Endpoint Security

Changing the Standby SMS to the Active SMS

1. When logging in to the Standby SMS, the Standby window is displayed.
2. In the displayed window, select **Change to Active**.

**Figure 11-29**  Change to Active

---

**Refreshing the Synchronization Status of the SMS**

If you suspect that the status of the Security Management server has changed, you may decide to do a refresh operation.

1. Display the Management High Availability Servers window for the selected SMS by selecting **Policy > Management High Availability**
2. In the displayed window, click **Refresh**.
Selecting the Synchronization Method

The manner in which the Standby SMSs synchronize with the Active SMS is defined in the Global Properties - Management High Availability window. This window is displayed by selecting Policy > Global Properties > Management High Availability. The Standby SMS can be synchronized automatically when the policy is installed, saved or on a specified scheduled event. Alternatively, the Standby SMS can be synchronized manually. If manual synchronization is the method of choice, the system administrator will need to initiate the manual synchronization in the Management High Availability Servers window. For more information, see Synchronization Modes (on page 149).

Tracking Management High Availability Throughout the System

The statuses of all the Security Management servers in the system are displayed in the Management High Availability window. This window is displayed by selecting Policy > Management High Availability. Details about the Security Management server and its peers that are displayed include the name, status and type of Security Management server.

All Management High Availability management operations can be viewed in the SmartView Tracker in Audit mode.
Chapter 12

Working with SNMP Management Tools

In This Chapter

The Need to Support SNMP Management Tools 156
The Check Point Solution for SNMP 156
Special Consideration for the Unix SNMP Daemon 158
Configuring Security Gateways for SNMP 158

The Need to Support SNMP Management Tools

SNMP management tools are used to monitor the activity of various devices on the network. Because system administrators prefer to work with familiar tools, they might feel more comfortable obtaining status information regarding Check Point products through their regular SNMP Network Management Station (NMS).

The Check Point Solution for SNMP

Check Point addresses this issue by running SNMP agents on Security Gateways. These Security Gateways need to respond to requests from an SNMP Management Station.

Figure 12-31 Basic SNMP deployment on a LAN

In the standard client-server relationship, the network SNMP Management Station is the client and the SNMP agent within the Check Point product acts as the server.
Understanding the SNMP MIB

SNMP management systems consist of an SNMP management station and the managed devices, such as bridges, routers, or network servers. SNMP agents constitute the software elements that interface with the device being managed. The agents relate to the configuration and performance characteristics of a managed device as separate identifiable objects. These objects are arranged in an hierarchical namespace, a tree-like database structure known as a Management Information Block, or MIB. Check Point has a registered MIB sub-tree with the Internet Assigned Numbers Authority (IANA). The MIB:

1. Gives structure to the data in the registered Check Point tree, assigning a unique number to a Check Point Security Gateway. The number, a string of integers separated by decimal points, is the OID or Object Identifier.
   - For Check Point, the root of the registered Object Identifier (OID) is 1.3.6.1.4.1.2620. The notation is: Check point OBJECT IDENTIFIER:: ={enterprises 2620}. For example, the MIB on the management station resolves a string such as 1.3.6.1.4.1.2640.1.1 to: iso.org.dod.internet.private.enterprises.checkpoint.products.fw.
   - The object definitions for Check Point are located in the Check Point MIB. The Check Point MIB can be read by any third party SNMP Management Station once the MIB has been imported.

2. Provides name resolution, resolving the OID integer string to a user-friendly name. For example, if an administrator wants to know the version number of a particular firewall, the administrator selects “version number” as the property of the managed device and the MIB maps “version number” to an integer string before sending the information request to the agent.

Note - The SNMP management station can read but not modify the object definitions for Check Point products.

Handling SNMP Requests on Windows

When the Security Management server is installed, a special Check Point dynamic link library (DLL) is listed in the Windows registry. The SNMP service running on the Operating System loads this DLL. The SNMP service listens in the standard way on port 161 for incoming SNMP requests from the SNMP Network Management Station. The Check Point DLL extends the Windows SNMP service to identify those status requests directed at Check Point products. The relevant data is then retrieved by the DLL and sent to the SNMP management station.

Note - The Check Point SNMP agent is an extension of the Windows SNMP agent. If you have not installed the standard Windows SNMP agent, you cannot use the Check Point SNMP agent.

Handling SNMP Requests on Unix

For the Unix platform, a special Check Point SNMP daemon, called cpsnmpd, is installed. This daemon provides status information on Check Point specific objects. This daemon is not run by default. The daemon is enabled or disabled through cpconfig. Once enabled, the daemon runs with other Check Point processes. The SNMP Network Management Station queries the daemon for status information. The daemon retrieves the information, and replies.

Note - While the Check Point daemon is SNMP compliant, the daemon listens on port 260 instead of 161. The standard Unix SNMP daemon loads before the Check Point daemon and binds to port 161. If the regular daemon is not running, cpsnmpd binds to both ports (161 and 260). If both ports are occupied by a previous process, the Check Point daemon will not run. Further, if the Check Point daemon receives an request for an unrecognized OID, it does not forward this to the standard snmp unix daemon.
Handling SNMP Requests on SecurePlatform

SNMP support is fully integrated in SecurePlatform:

- Net-SNMP Support for full OS-MIB-II.
- Monitoring of Check Point Status Information (AMON) through SNMP.
- SNMP V.2 and V.3 Support.


SNMP Traps

While Check Point has Alert as one of its tracking types, you might prefer to receive alert messages through your regular SNMP Management Station in the form of an SNMP trap. An SNMP trap is notification that a certain event has occurred. Check Point offers SNMP traps as one of its tracking types. When the conditions of the trap are met, the gateway sends a log to Security Management server. Security Management server saves the log and sends (via port 162) an SNMP trap to the configured catcher—the SNMP Network Management station. The trap includes the text of the log file.

For example, if any machine outside of the organization tries to make an http connection to a machine within the internal network, the packet is dropped and an SNMP trap is sent:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Internal_private_network</td>
<td>Any</td>
<td>HTTP</td>
<td>Drop</td>
<td>SnmpTrap</td>
</tr>
</tbody>
</table>

Special Consideration for the Unix SNMP Daemon

If you need to run the standard Unix SNMP daemon on port 161, run this daemon before you start cpsnmpd, otherwise cpsnmpd will take the port.

Configuring Security Gateways for SNMP

To handle SNMP requests and traps, the various supported platforms need to be configured in slightly different ways.

Configuring Security Gateways for SNMP Requests

1. On the SNMP Management Station, import the Check Point MIB file from $CPDIR/lib/snmp/chkpnt.mib.
2. If the platform is Windows NT, verify that the Operating System is running the SNMP service. On the Unix platform, verify that port 260 is not bound to another process. If port 260 is available, run cpconfig to enable the cpsnmpd daemon.
3. In the Security Policy Rule Base:
   - Open port 161 if the platform is Windows NT.
   - Open port 260 if the platform is Unix.
Do this only on the Security Gateways through which the SNMP packets need to pass.

**Figure 12-32** Allowing SNMP packets through Security Gateways

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>Proto</th>
<th>SERVICE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SNMP_Management_Station</td>
<td>Firewall_Modules</td>
<td>Any</td>
<td>snmp</td>
<td>accept</td>
</tr>
</tbody>
</table>

This policy rule allows the SNMP Management Station to communicate with the Security Gateways.

4. Install the new Security Policy.

**Configuring Security Gateways for SNMP Traps**

To configure Security Gateways for SNMP traps, the built-in trap script has to be assigned an appropriate catcher.

**To assign an appropriate catcher:**
1. Open the Global Properties window, Alert Commands page.
2. Select the Run SNMP trap alert script option.
3. In the corresponding text box, replace `internal_snmp_trap localhost` with `internal_snmp_trap <snmp_trap_catcher>`, where the `<variable>` is replaced with the name of the configured catcher. For example, if the configured catcher is a machine called Alaska, the new script would read `internal_snmp_trap Alaska`.

4. For the relevant rules in the Security Policy Rule Base, set the tracking type to `snmp_trap`. 

![Global Properties window with Alert Commands](image)
5. If Security Management server and the SNMP Management Station do not reside on the same network segment, open port 162 on all Security Gateways between them. This will allow SNMP traps to pass through.

Figure 12-33 Assigning a trap catcher

6. Install the Security Policy.
Chapter 13

Security Management Servers on DHCP Interfaces

In This Chapter

Requirements 161
Enabling and Disabling 161
Using a Dynamic IP Address 161
Licensing a Dynamic Security Management Server 162
Limitations for a Dynamic Security Management Server 162

Requirements

Beginning with version R71, Security Management Servers are supported with Dynamic IP addresses on DHCP. To use this:

- The Security Management Server must be on a Windows system with a DHCP adapter.
- The Security Management Server must be part of a distributed deployment.

Enabling and Disabling

When you install a Security Management Server on a Windows machine with a DHCP interface, the Security Management Server recognizes the DHCP interface. As a result, a Dynamic Address checkbox appears in the General Properties of the Security Management Server object. This checkbox is automatically selected to enable using the Security Management Server with a dynamic IP address.

If the Security Management Server object is not shown in SmartDashboard, make sure that at least one interface is defined with a valid IP address and run cpstop and cpstart to restart Check Point services.

Clear the checkbox to disable the feature and to indicate that a static IP address is being used. When the Dynamic Address checkbox is cleared, Security Gateways will only accept connections from the exact last known IP address of the Security Management Server.

Using a Dynamic IP Address

For the Security Management Server to install policy, it should use an IP address that is defined as an allowed Network or Address Range. If no range is defined, a default address range is created from the first 3 octets of the first assigned IP address. For example, if the server is configured with the IP address 192.168.184.55, the default range will be 192.168.184.0 - 192.168.184.255. You can define a new allowed address network or range at any time.

When the managed Security Gateway is of version R71, policy installation fails if the IP address of the Security Management Server is outside of the defined ranges and networks.

When the IP address of the Security Management Server changes, the change is reflected in the database after you restart the SmartDashboard.
To define an allowed Network or Address Range:
1. From the General Properties window of the Security Management Server object, click Manage. The Management DHCP Ranges window opens.
2. Click Add to add a new Network or Address Range.
   - Network - Define the first IP address and a subnet mask
   - Address Range - Define the first and last IP address of the range.
3. When all networks and address ranges are added, click OK to activate them.

Licensing a Dynamic Security Management Server

A Security Management Server uses constant IP address based on a MAC address.

To obtain a license for a Security Management Server with a dynamic IP address:
1. Run cplic dynlic from the CLI. An IP address is returned.
2. Use this IP address to obtain a license from the Check Point User Center (http://usercenter.checkpoint.com).
3. Run cplic put in the CLI to install the license. Do not install it using SmartUpdate.

Limitations for a Dynamic Security Management Server

- You cannot configure a Security Management Server on a DHCP interface in a standalone deployment.
- A dynamic Security Management Server can only manage remote UTM-1 gateways, Power-1 gateways, and IPS-1 Sensors if they have static IP addresses and are of version R70 or higher.
- Management High Availability is not supported together with automatic IP Address replacement of the Security Management Server.
Appendix A

Network Objects

In This Appendix

| Introduction to Objects | 163 |
| Network Objects         | 164 |

Introduction to Objects

Network Objects are created in order to represent actual physical machines and components such as gateway, servers, as well as logical components such as IP Address Ranges and Dynamic Objects.

Objects are created and managed by the system administrator via SmartDashboard.

All objects are managed using SmartDashboard; therefore, it is recommended that the objects database must not be accessed or edited directly. In this appendix you will find general information about network objects, including configuration specifications, where necessary.

The Objects Creation Workflow

1. Objects created by the system administrator, are automatically stored in the objects database on the Security Management server in $FWDIR/conf/objects_5_0.c.
2. When the Security Policy is installed on the Security Gateway, Security Management server computes the objects.c file for the Security Gateway. This file is computed and derived from the objects_5_0.c file.
4. When a policy is installed, all changes made to objects are applied and saved. These changes are also registered in the objects database which is automatically updated.

Viewing and Managing Objects

When an object is created it is allocated an iconic representation that can be viewed and applied from any of the following locations:

- **Objects Tree** is the Objects manager from which objects are created, viewed and managed. To make sure that all network objects folders are displayed, right-click on the Network Objects root, and uncheck Do not show empty folders.
- **Objects List** is the view from which detailed information about specific objects categories is displayed (such as all the available networks).
- **Rule Base** is the view in which objects are implemented and applied to the rules which make up the Security Policy.
- **SmartMap** is the view in which the objects implemented in the Rule Base are displayed in a graphical representation.
Network Objects

Check Point Objects

Security Gateways

A Security Gateway object is a gateway with more than one interface on which Check Point Software Blades are installed. At least a firewall blade is installed, although other Check Point Software Blade such as QoS or Monitoring may also be installed. This gateway sits on the network that serves as an entry point to the LAN and is managed by the Security Management server. A Security Gateway is characterized as follows:

- it has one or more Software Blades installed
- where the IPSec VPN blade is installed, it requires a VPN license
- it is a routing mechanism that is capable of IP forwarding
- since it has more than one interface it can be used in order to implement anti-spoofing.

If the Security Gateway that you defined does not need to perform IP forwarding or anti-spoofing, you can convert it to a Check Point host.

Converting a Security Gateway into a Check Point host

You can convert a Security Gateway to a Check Point host by right-clicking the Security Gateway in the Objects Tree and selecting Convert to Host.

UTM-1 Edge Gateway

A UTM-1 Edge gateway object is a network object that represents a UTM-1 Edge gateway. This gateway sits on the network and can be managed by the Security Management server or by an external management server.

Defining UTM-1 Edge Gateway Objects

1. In the Network Objects tab of the Objects Tree, create a new UTM-1 Edge gateway.
2. Configure the general settings of the window, including its name and IP address (whether static or dynamic) and version information.
3. To define the UTM-1 Edge gateway as a member of a VPN community, select the VPN Enabled check box and select the VPN Community type (whether Site to Site or Remote Access).

Check Point Host

A Check Point host is a host with only one interface, on which Check Point software has been installed, and which is managed by the Security Management server.

A Check Point host is characterized as follows:

- It has one or more Check Point Software Blades installed.
- It is not a routing mechanism and is not capable of IP forwarding.
- Since it only has one interface, its topology cannot be modified and therefore it cannot be used to implement Anti-spoofing.
- It requires a SecureServer license and not a VPN license.

If you have defined a Check Point host and you are trying to use it to perform IP forwarding or anti-spoofing, you must convert it to a Security Gateway.

Converting a Check Point host into a Security Gateway

You can convert a Check Point host to a Security Gateway by right-clicking the Check Point host in the Objects Tree and selecting Convert to Gateway.
**Gateway Cluster**

A gateway cluster is a group of Security Gateway machines on which Check Point software has been installed which have been configured to provide failover services using ClusterXL or another Cluster solution.

**Converting a Cluster Member into a Security Gateway**

You can detach a Cluster member from a gateway cluster and convert it into a Security Gateway as follows:

1. Right-click on a Cluster object in the Objects Tree or List.
2. Select **Detach Cluster Members** from the menu.
3. Select the member from the displayed window and click **Detach**.
4. Ignore the displayed warning in order to complete the conversion.
5. The gateway Properties window of the converted cluster member is displayed. Click **OK** to finalize the conversion.

**Externally Managed Gateway/Host**

An Externally Managed Security Gateway or Host is a gateway or Host which has been installed with Check Point software. This Externally Managed gateway is a Security Gateway which is managed by an external Security Management server. While it does not receive the Check Point Security Policy, it can participate in Check Point VPN communities and solutions.

**Nodes**

A node can represent any network entity. The two most common uses of this object are to create non-Security Gateways and Hosts.

- A gateway node is a gateway which does not have Check Point software installed.
- A host node is a host which does not have Check Point software installed.

**Converting Nodes**

- Gateway Nodes can be converted to Host Nodes and *vice versa*. Right-click on the specified Node in the Objects Tree and selecting **Convert to Host** or **Gateway**.
- Gateway Nodes can be converted to Security Gateways. Right-click on the gateway Node in the Objects Tree and select **Convert to Check Point Gateway**.
- Host Nodes can be converted to Check Point hosts. Right-click on the specified Host Node in the Objects Tree and select **Convert to Check Point Host**.

**Interoperable Device**

An Interoperable Device is a device which has no Check Point Software Blades installed. This device is managed by any Management Server, including Security Management server, although it cannot receive the Check Point Security Policy, and it can participate in Check Point VPN communities and solutions.

**Networks**

A Network is a group of IP addresses defined by a network address and a net mask. The net mask indicates the size of the network.

A Broadcast IP address is an IP address which is destined for all hosts on the specified network. If this address is included, the Broadcast IP address will be considered as part of the network.

**Domains**

This object defines a DNS domain name.
The format of the domain name is .x.y, where each section of the domain name is demarcated by a period. For instance .mysite.com or .mysite.co.uk. The domain name that is specified must be an actual domain name in order that it can be resolved to a valid IP address. The first time that a domain name is resolved by the Security Management server a brief delay may occur. Once the domain name has been resolved it is entered into the cache, and no further delays will take place on any subsequent access attempts. On account of the initial delays which may occur for each new domain name, the rules that contain Domain objects in their Source or Destination should be placed towards the end of the Rule Base.

Open Security Extension (OSE) Devices

Overview to OSE Devices

The Open Security Extension features enables Check Point to manage third-party open security extension devices (OSE). The number of managed devices depends on your license. Devices include hardware and software packet filters. Check Point also supports hardware security devices which provide routing and additional security features, such as Network Address Translation and Authentication. Security devices are managed in the Security Policy as Embedded Devices. The Security Management server generates Access Lists from the Security Policy and downloads them to selected routers and open security device. Check Point supports the following devices, as shown in the following table:

Table 13-10  **Check Point Supported OSE Devices**

<table>
<thead>
<tr>
<th>OSE Device</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Systems</td>
<td>9.x, 10.x, 11.x, 12.x</td>
</tr>
<tr>
<td>Nortel</td>
<td>13.x, 14.x</td>
</tr>
</tbody>
</table>

When working with a Cisco Router (that is, OSE object), the Rule Base should not contain one of the following. If one of the following is included in the Rule Base, the Security Management server will fail to generate Access Lists from the rules.

- Drop (in the Action column)
- Encrypt (Action)
- Alert (Action)
- RPC (Service)
- <??AH>(Service)
- ACE (Service)
- Authentication Rules
- Negate Cell

OSE Device Properties Window — General Tab

- **Name** — the name of the OSE device
  The name given here should be identical to the name as it appears in the system database on the server.
- **IP Address** — the device’s IP address
- **Get Address** — click this button to resolve the name to an address
  
  **Note** - It is recommended that you list OSE device objects in your hosts (Unix) and lmhosts (Windows) files in addition to defining them in the Check Point database.
- **Comment** — This text is displayed on the bottom of the **Network Object** window when this object is selected.
- **Color** — Select a color from the drop-down list. The OSE device will be represented in the color selected throughout the SmartMap for easier user tracking and management.
- **Type** — choose one of the following from the drop-down menu:
OSE devices report their network interfaces and setup at boot time. Each OSE device has a different command for listing its configuration.

**Note** - At least one interface must be defined in the Topology tab or Install Policy will fail.

To add an interface, click Add. The Interface Properties window is displayed.

To edit an interface, select the interface and click Edit, or double-click the interface. The Interface Properties window is displayed.

To delete an interface, select the interface and click Remove.

The manner in which names are specified for OSE device interfaces is different from the manner in which they are specified for interfaces of other network objects.

- **Name** — name of the network interface as specified in the router's interface configuration scheme. This name does not include a trailing number.

- **IP Address** — the IP address of the device

- **Net Mask** — the net mask of the device.

**Defining Router Anti-Spoofing Properties**

The Interface Properties window allows you to define router anti-spoofing parameters when installing Access Lists on routers. The Interface Properties window is almost identical to the Interface Properties window for network objects.

**Note** - To implement anti-spoofing for Cisco (version 10.x and higher), you must define additional properties in the Setup tab of each router after you define the Valid Addresses in the Interfaces Properties window. For more information, see Anti-spoofing Parameters and OSE Devices Setup (Cisco and Nortel) (on page 167).

**Note** - Logging for spoofing attempts is available for external interfaces only.

**Anti-spoofing Parameters and OSE Devices Setup (Cisco and Nortel)**

For Cisco (Version 10.x and higher) and Nortel OSE devices, you must specify the direction of the filter rules generated from anti-spoofing parameters. The direction of enforcement is specified in the Setup tab of each router.

For Cisco routers, the direction of enforcement is defined by the Spoof Rules Interface Direction property.

- **Access List No** — the number of Cisco access lists enforced.

- **Username** — the name required to logon to the OSE device.

- **Password** — the Administrator password (Read only) as defined on the router.

- **Enable Username** — the user name required to install Access Lists.

- **Enable Password** — the password required to install Access Lists.
The security administrator must select one of the following options from the drop-down list for the above **Username** and **Password** fields (this includes the Enable fields):

- **None** — Indicates the parameter is not needed.
- **Known** — the value of the parameter must be entered.
- **Prompt** — Indicates that the security administrator will be prompted for this parameter.

**Version** — the Cisco OSE device version (9.x, 10.x, 11.x, 12.x).

**OSE Device Interface Direction** — Installed rules are enforced on data packets traveling in this direction on all interfaces.

**Spoof Rules Interface Direction** — The spoof tracking rules are enforced on data packets traveling in this direction on all interfaces.

---

**Groups**

A network objects group is a collection of hosts, gateways, networks or other groups.

Groups are used in cases where you cannot work with single objects, e.g. when working with VPN domains or with topology definitions.

In addition, groups can greatly facilitate and simplify network management, since they allow you to perform operations only once instead of repeating them for every group member.

The **Group Properties** window lists the network objects included from the group versus those excluded from the group. To configure the group, move objects between the lists as needed.

To include an unlisted network object in the group, create it now by clicking **New**.

This window shows collapsed sub-groups, without listing their members. For a list of all group members (including the sub-groups’ members), click **View Expanded Group**.

---

**Logical Servers**

A Logical Server is a group of machines that provides the same services. The workload of this group is distributed between all its members.

When a Server group is stipulated in the **Servers group** field, the client is bound to this physical server. In Persistent server mode the client and the physical server are bound for the duration of the session.

- **Persistency by Service** — once a client is connected to a physical server for a specified service, subsequent connection to the same Logical Server and the same service will be redirected to the same physical server for the duration of the session.

- **Persistency by Server** — once a client is connected to a physical server, subsequent connections to the same Logical Server (for any service) will be redirected to the same physical server for the duration of the session.

---

**Balance Method**

The load balancing algorithm stipulates how the traffic is balanced between the servers. There are several types of balancing methods:

- **Server Load** — The Security Gateway determines which Server is best equipped to handle the new connection.

- **Round Trip Time** — On the basis of the shortest round trip time between Security Gateway and the servers, executed by a simple ping, the Security Gateway determines which Server is best equipped to handle the new connection.

- **Round Robin** — the new connection is assigned to the first available server.

- **Random** — the new connection is assigned to a server at random.

- **Domain** — the new connection is assigned to a server based on domain names.
Network Objects

Address Ranges
An Address Range object stipulates the range of IP addresses used in the network from the first to the last IP address.
This object is used when the networks themselves do not have IP address-net mask alignment, so an Address Range is necessary for the implementation of:
- NAT, and
- VPN

Dynamic Objects
A dynamic object is a "logical" object where the IP address will be resolved differently per Security Gateway using the dynamic_objects command.
The following are the predefined Dynamic Objects:
- **LocalMachine-all-interfaces** – The DAIP machine interfaces (static and dynamic) are resolved into this object.
- **LocalMachine** – The external interface (dynamic) of the ROBO gateway (as declared in cpconfig when configuring the ROBO gateway).
- **InternalNet** – The internal interface of the ROBO gateway (as declared in cpconfig when configuring the ROBO gateway).
- **AuxiliaryNet** – The auxiliary interface of the ROBO gateway (as declared in cpconfig when configuring the ROBO gateway).
- **DMZNet** – The DMZ interface of the ROBO gateway (as declared in cpconfig when configuring the ROBO gateway).

For more information see the [R71 Command Line Interface Reference Guide](http://supportcontent.checkpoint.com/documentation_download?id=10324).

VoIP Domains
There are five types of VoIP Domain objects:
- VoIP Domain SIP Proxy
- VoIP Domain H.323 Gatekeeper
- VoIP Domain H.323 Gateway
- VoIP Domain MGCP Call Agent
- VoIP Domain SCCP CallManager

In many VoIP networks, the control signals follow a different route through the network than the media. This is the case when the call is managed by a signal routing device. Signal routing is done in SIP by the Redirect Server, Registrar, and/or Proxy. In SIP, signal routing is done by the Gatekeeper and/or gateway.

Enforcing signal routing locations is an important aspect of VoIP security. It is possible to specify the endpoints that the signal routing device is allowed to manage. This set of locations is called a VoIP Domain.

Appendix B

CLI Appendix


Table 13-11 Security Management server Command Line Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpca_client</td>
<td>This command and all its derivatives are used to execute operations on the ICA.</td>
</tr>
<tr>
<td>cpca_client create_cert</td>
<td>This command prompts the ICA to issue a SIC certificate for the Security Management server.</td>
</tr>
<tr>
<td>cpca_client revoke_cert</td>
<td>This command is used to revoke a certificate issued by the ICA.</td>
</tr>
<tr>
<td>cpca_client set_mgmt_tools</td>
<td>This command is used to invoke or terminate the ICA Management Tool.</td>
</tr>
<tr>
<td>cpconfig</td>
<td>This command is used to run a Command Line version of the Check Point Configuration Tool. This tool is used to configure/reconfigure a Check Point installation.</td>
</tr>
<tr>
<td>cplic</td>
<td>This command and all its derivatives relate to the subject of Check Point license management. All cplic commands are located in $CPRID/bin.</td>
</tr>
<tr>
<td>cplic check</td>
<td>Use this command to check whether the license on the local machine will allow a given feature to be used.</td>
</tr>
<tr>
<td>cplic db_add</td>
<td>The cplic db_add command is used to add one or more licenses to the license repository on the Security Management server. When local license are added to the license repository, they are automatically attached to its intended Security Gateway, central licenses need to undergo the attachment process.</td>
</tr>
<tr>
<td>cplic db_print</td>
<td>The cplic db_print command displays the details of Check Point licenses stored in the license repository on the Security Management server.</td>
</tr>
<tr>
<td>cplic db_rm</td>
<td>The cplic db_rm command removes a license from the license repository on the Security Management server. It can be executed ONLY after the license was detached using the cplic del command. Once the license has been removed from the repository, it can no longer be used.</td>
</tr>
<tr>
<td>cplic del</td>
<td>Use this command to delete a single Check Point license on a host, including unwanted evaluation, expired, and other licenses. This command is used for both local and remote machines.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cplic del &lt;object name&gt;</td>
<td>Use this command to detach a Central license from a Security Gateway. When this command is executed, the License Repository is automatically updated. The Central license remains in the repository as an unattached license. This command can be executed only on a Security Management server.</td>
</tr>
<tr>
<td>cplic get</td>
<td>The cplic get command retrieves all licenses from a Security Gateway (or from all Security Gateways) into the license repository on the Security Management server. Do this to synchronize the repository with the Security Gateway (or with all the Security Gateways). When the command is run, all local changes will be updated.</td>
</tr>
<tr>
<td>cplic put</td>
<td>The cplic put command is used to install one or more Local licenses on a local machine.</td>
</tr>
<tr>
<td>cplic put &lt;object name&gt;</td>
<td>Use the cplic put command to attach one or more central or local license remotely. When this command is executed, the License Repository is also updated.</td>
</tr>
<tr>
<td>cplic print</td>
<td>The cplic print command (located in $CPDIR/bin) prints details of Check Point licenses on the local machine.</td>
</tr>
<tr>
<td>cplic upgrade</td>
<td>Use the cplic upgrade command to upgrade licenses in the license repository using licenses in a license file obtained from the User Center.</td>
</tr>
</tbody>
</table>
| cp_merge      | This utility has two main functionalities:  
Export and import of policy packages  
Merge of objects from a given file into the Security Management server database |
<p>| cp_merge delete_policy | This command provides the options of deleting an existing policy package. Note that the default policy can be deleted by delete action. |
| cp_merge export_policy | This command provides the options of leaving the policy package in the active repository, or deleting it as part of the export process. The default policy cannot be deleted during the export action. |
| cp_merge import_policy|restore_policy | This command provides the options to overwrite an existing policy package with the same name, or prevent overwriting when the same policy name already exists. |
| cp_merge list_policy | This command lists the Policy Packages that are available. |
| cppkg         | This command is used to manage the Package Repository. It is always executed on the Security Management server.                                |
| cppkg add     | The cppkg add command is used to add a package to the Package Repository. Only packages can be added to the Package Repository.               |
| cppkg delete  | The command is used to delete a package from the Package Repository. To delete a package you must specify a number of options. To see the format of the options and to view the contents of the Package Repository, use the cppkg print command. |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cppkg get</td>
<td>This command synchronizes the Package Repository database with the content of the actual Package Repository under $SUROOT.</td>
</tr>
<tr>
<td>cppkg getroot</td>
<td>The command is used to find out the location of the Package Repository. The default Package Repository location on Windows machines is C:\SUroot. On UNIX it is /var/SUroot.</td>
</tr>
<tr>
<td>cppkg print</td>
<td>The command is used to list the contents of the Package Repository.</td>
</tr>
<tr>
<td>cppkg setroot</td>
<td>The command is used to create a new repository root directory location, and to move existing packages into the new Package Repository.</td>
</tr>
<tr>
<td>cpridrestart</td>
<td>Stops and starts the Check Point Remote installation Daemon (cprid). This is the daemon that is used for remote upgrade and installation of products. It is part of the SVN Foundation. In Windows it is a service.</td>
</tr>
<tr>
<td>cpridstart</td>
<td>Starts the Check Point Remote installation Daemon (cprid). This is the service that allows for the remote upgrade and installation of products. It is part of the SVN Foundation. In Windows it is a service.</td>
</tr>
<tr>
<td>cpridstop</td>
<td>Stops the Check Point Remote installation Daemon (cprid). This is the service that allows for the remote upgrade and installation of products. It is part of the SVN Foundation. In Windows it is a service.</td>
</tr>
<tr>
<td>cprinstall</td>
<td>Use cprinstall commands to perform remote installation of packages, and associated operations.</td>
</tr>
<tr>
<td>cprinstall boot</td>
<td>This command is used to boot the remote computer.</td>
</tr>
<tr>
<td>cprinstall cprestart</td>
<td>This command enables cprestart to be run remotely.</td>
</tr>
<tr>
<td>cprinstall cpstart</td>
<td>This command enables cpstart to be run remotely.</td>
</tr>
<tr>
<td>cprinstall cpstop</td>
<td>This command enables cpstop to be run remotely.</td>
</tr>
<tr>
<td>cprinstall get</td>
<td>The cprinstall get command is used to obtain details of the packages and the Operating System installed on the specified Security Gateway, and to update the database.</td>
</tr>
<tr>
<td>cprinstall install</td>
<td>The cprinstall install command is used to install Check Point packages, UTM-1 Edge firmware packages, OPSEC partner packages (SU compliant) and Check Point IPSO images on remote Security Gateways. To install a package you must specify a number of options. Use the cppkg print command and copy the required options.</td>
</tr>
<tr>
<td>cprinstall uninstall</td>
<td>The cprinstall uninstall command is used to install Check Point packages, UTM-1 Edge firmware packages, OPSEC partner packages (SU compliant) and Check Point IPSO images on remote Security Gateways. To uninstall a package you must specify a number of options. Use the cprinstall get command and copy the required options.</td>
</tr>
</tbody>
</table>
### Command | Description
--- | ---

cprinstall verify | The cprinstall verify command is used to verify:
- If a specific product can be installed on the remote Security Gateway.
- That the Operating System and currently installed products are appropriate for the package.
- That there is enough disk space to install the product.
- That there is a CPRID connection.

cpstart | This command is used to start all Check Point processes and applications running on a machine.

cpstat | cpstat displays the status of Check Point applications, either on the local machine or on another machine, in various formats.

cpstop | This command is used to terminate all Check Point processes and applications running on a machine.

cpwd_admin | cpwd (also known as WatchDog) is a process that invokes and monitors critical processes such as Check Point daemons on the local machine, and attempts to restart them if they fail. Among the processes monitored by Watchdog are cpd, fwd, fwm. cpwd is part of the SVN Foundation.

- cpwd writes monitoring information to the `$CPDIR/log/cpwd.elg` log file. In addition, monitoring information is written to the console on UNIX platforms, and to the Windows Event Viewer.

- The cpwd_admin utility is used to show the status of processes, and to configure cpwd.

cpwd_admin config | This command is used to set cpwd configuration parameters. When parameters are changed, these changes will not take affect until cpwd has been stopped and restarted.

cpwd_admin exist | This command is used to check whether cpwd is alive.

cpwd_admin kill | This command is used to kill cpwd.

cpwd_admin list | This command is used to print a status of the selected processes being monitored by cpwd.

cpwd_admin monitor_list | This command is used to print the list of processes actively being monitored.

cpwd_admin start | Start a new process by cpwd.

cpwd_admin start_monitor | This command is used to start continuous monitoring on this machine.

cpwd_admin stop | Stop a process which is being monitored by cpwd.

cpwd_admin stop_monitor | This command is used to stop continuous monitoring on this machine.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbedit</td>
<td>This command is used by administrators to edit the objects file on the Security Management server. There is an objects file on the gateway and a file, objects_5_0.C on the Security Management server. A new objects.C file is created on the gateway (based on the objects_5_0.C on the Security Management server) whenever a Policy is installed. Editing the objects.C file on the gateway is not required or desirable, since it will be overwritten the next time a Policy is installed.</td>
</tr>
<tr>
<td>DBTableStat</td>
<td>This utility provides a daily summary of the number of log records that match the consolidation rules, and the number of consolidated records that were stored in the specified database table. The format of the output is a comma separated value. The execution time of this utility depends on the number of records in the SmartReporter table.</td>
</tr>
<tr>
<td>dbver</td>
<td>The dbver utility is used to export and import different revisions of the database. The properties of the revisions (last time created, administrator responsible for, etc.) can be reviewed. The utility can be found in $FWDIR/bin.</td>
</tr>
<tr>
<td>dbver create</td>
<td>Create a revision from the current state of $fwdir/conf, including current objects, rule bases, etc.</td>
</tr>
<tr>
<td>dbver export</td>
<td>Archive the revision as an archive file in the revisions repository: $fwdir/conf/db_versions/export.</td>
</tr>
<tr>
<td>dbver import</td>
<td>Add an exported revision to the repository a version from $fwdir/conf/db_versions/export. Give filename of revision as input.</td>
</tr>
<tr>
<td>dbver print</td>
<td>Print the properties of the revision.</td>
</tr>
<tr>
<td>dbver print_all</td>
<td>Print the properties of all revisions to be found on the server side: $fwdir/conf/db_versions.</td>
</tr>
<tr>
<td>dynamic_objects</td>
<td>dynamic_objects specifies an IP address to which the dynamic object will be resolved on this machine.</td>
</tr>
<tr>
<td>fw</td>
<td>The fw commands are used for working with various aspects of the firewall component of the Security Gateway. All fw commands are executed on the gateway. Typing fw at the command prompt sends a list of available fw commands to the standard output.</td>
</tr>
<tr>
<td>fw ctl</td>
<td>The fw ctl command controls the Security Gateway kernel.</td>
</tr>
<tr>
<td>fw expdate</td>
<td>This command is used to modify the expiration date of all users and administrators.</td>
</tr>
<tr>
<td>fw fetch</td>
<td>This command fetches the Inspection Code from the specified host and installs it to the kernel.</td>
</tr>
<tr>
<td>fw fetchlogs</td>
<td>fw fetchlogs fetches Log Files from a remote machine. You can use the fw fetchlogs command to transfer Log Files to the machine on which the fw fetchlogs command is executed. The Log Files are read from and written to the directory $FWDIR/log.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fw hastat</td>
<td>The <em>fw hastat</em> command displays information about High Availability machines and their states.</td>
</tr>
<tr>
<td>fw kill</td>
<td>This command prompts the kernel to shut down all the daemon processes in the firewall component of the Security Gateway. The command is located in the $FWDIR/bin directory on the Security Management server or gateway. The Security Gateway daemons and Security Servers write their pids to files in the $FWDIR/tmp directory upon startup. These files are named $FWDIR/tmp/daemon_name.pid. For example, the file containing the pid of the Security Gateway snmp daemon is $FWDIR/tmp/snmpd.pid.</td>
</tr>
<tr>
<td>fw lea_notify</td>
<td>This command should be run from the Security Management server. It sends a LEA_COL_LOGS event to all connected lea clients (see the LEA Specification documentation). It should be used after new log files have been imported (manually or automatically) to the $FWDIR/log directory in order to avoid the scheduled update which takes 30 minutes.</td>
</tr>
<tr>
<td>fw lichosts</td>
<td>This command prints a list of hosts protected by the Security Gateways. The list of hosts is in the file $fwdir/database/fwd.h</td>
</tr>
<tr>
<td>fw log</td>
<td><em>fw log</em> displays the content of Log files.</td>
</tr>
<tr>
<td>fw logswitch</td>
<td><em>fw logswitch</em> creates a new active Log File. The current active Log File is closed and renamed by default $FWDIR/log/current_time_stamp.log unless you define an alternative name that is unique. The format of the default name current_time_stamp.log is YYYY-MM-DD_HHMMSS.log. For example: 2003-03-26_041200.log</td>
</tr>
<tr>
<td>fw mergefiles</td>
<td>This command merges several Log Files into a single Log File. The merged file can be sorted according to the creation time of the Log entries, and the times can be &quot;fixed&quot; according to the time zones of the origin Log Servers. When the combined size exceeds 2GB, the merge creates a list of &quot;merged files&quot; where each file size is not more than 2GB. The user receives the following warning: &quot;Warning: The size of the files you have chosen to merge is greater than 2GB. The merge will produce two or more files.&quot; The files names will be: [Requested name].log, [Requested name]_1.log, [Requested name]_2.log, ...,[Requested name]_n.log. Log entries with the same Unique-ID are unified. If a Log switch was performed before all the segments of a specific log were received, this command will merge the records with the same Unique-ID from two different files into one fully detailed record.</td>
</tr>
<tr>
<td>fw lslogs</td>
<td>This command displays a list of Log Files residing on a remote or local machine. You must initialize SIC between the Security Management server and the remote machine.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fw putkey</td>
<td>This command installs an authentication password on a host. This password is used to authenticate internal communications between Check Point Security Gateways and between a Check Point Security Gateway and its Security Management server. A password is used to authenticate the control channel the first time communication is established. This command is required for backward compatibility scenarios.</td>
</tr>
<tr>
<td>fw repairlog</td>
<td>fw repairlog rebuilds a Log file’s pointer files. The three files name.logptr, name.loginitial_ptr and name.logaccount_ptr are recreated from data in the specified Log file. The Log file itself is modified only if the -u flag is specified.</td>
</tr>
<tr>
<td>fw sam</td>
<td>This command is used to manage the Suspicious Activity Monitoring (SAM) server. Use the SAM server to block connections to and from IP addresses without the need to change the Security Policy. SAM commands are logged. Use this command to (also) monitor active SAM requests (see -M option).</td>
</tr>
<tr>
<td></td>
<td>To configure the SAM Server on the Security Management server or firewall gateway machine, use SmartDashboard to edit the Advanced&gt;SAM page of the Security Gateway object.</td>
</tr>
<tr>
<td>fwm</td>
<td>This command is used to perform Security Management server operations. It controls fwd and all Check Point daemons.</td>
</tr>
<tr>
<td>fwm dbimport</td>
<td>fwm dbimport imports users into the Security Management server User Database from an external file. You can create this file yourself, or use a file generated by fwm dbexport.</td>
</tr>
</tbody>
</table>
| fwm dbexport | fwm dbexport exports the Security Management server User Database to a file. The file may be in one of the following formats:  
- The same Usage as the import file for fwm dbimport  
- LDIF format, which can be imported into an LDAP Server using ldapmodify                                                                                                                                                                                                                                      |
<p>| fwm dbload | This command downloads the user database and network objects information to selected targets. If no target is specified, then the database is downloaded to localhost.                                                                                                                                                                                                                                                                                         |
| fwm ikecrypt | fwm ikecrypt command line encrypts the password of a SecuRemote user using IKE. The resulting string must then be stored in the LDAP database.                                                                                                                                                                                                                                                                                                      |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fwm load</td>
<td>This command compiles and installs a Security Policy or a specific version of the Security Policy on the target's VPN Security Gateways. This is done in one of two ways:</td>
</tr>
<tr>
<td></td>
<td>- fwm load compiles and installs an Inspection Script (*.pf) file on the designated Security Gateways.</td>
</tr>
<tr>
<td></td>
<td>- fwm load converts a Rule Base (<em>.W) file created by the GUI into an Inspection Script (</em>.pf) file then installs it to the designated Security Gateways.</td>
</tr>
<tr>
<td></td>
<td>Versions of the Security Policy and databases are maintained in a version repository on the Security Management server. Using this command, specific versions of the Security Policy can be installed on a Security Gateway (local or remote) without changing the definition of the current active database version on the Security Management server.</td>
</tr>
<tr>
<td></td>
<td>To protect a target, you must load a Policy that contains rules whose scope matches the target. If none of the rules are enforced on the target, then all traffic through the target is blocked.</td>
</tr>
<tr>
<td>fwm lock_admin</td>
<td>This command enables you to view and unlock locked administrators.</td>
</tr>
<tr>
<td>fwm logexport</td>
<td>fwm logexport exports the Log file to an ASCII file.</td>
</tr>
<tr>
<td>fwm unload &lt;targets&gt;</td>
<td>This command uninstalls the currently loaded Inspection Code from selected targets.</td>
</tr>
<tr>
<td>fwm ver</td>
<td>fwm ver displays the build number.</td>
</tr>
<tr>
<td>fwm verify &lt;policy-name&gt;</td>
<td>This command verifies the specified Policy Package without installing it.</td>
</tr>
<tr>
<td>GeneratorApp</td>
<td>This command generates a report for the SmartReporter. Both command line parameters are required.</td>
</tr>
<tr>
<td>inet_alert</td>
<td>This command notifies a company's Internet Service Provider (ISP) when the company's corporate network is under attack. The inet_alert utility forwards log messages generated by the alert daemon to an external Security Management server, typically located at the ISP site. The ISP can then analyze the alert and decide how to react.</td>
</tr>
<tr>
<td></td>
<td>inet_alert uses the ELA Protocol to send the alert. The Security Management server receiving the alert must be running the ELA Proxy.</td>
</tr>
<tr>
<td></td>
<td>If communication with the ELA Proxy is to be authenticated or encrypted, a key exchange must be performed between the Security Management server running the ELA Proxy and the gateway generating the alert.</td>
</tr>
<tr>
<td></td>
<td>To use this utility, enter it into a script. From Global Properties &gt; Logs and alert &gt; alert commands and enter the name of the script.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldapcmd</td>
<td>ldapcmd is used to manage processes running on the firewall collectively or individually. It includes: Cache - cache operations, such as emptying the cache, as well as providing debug information. Statistics - lookup statistics such as all user search, pending lookups (when two or more lookups are identical) and total lookup time (the total search time for a specific lookup) cache statistics such as hits and misses Logging - view the alert and warning log regarding debug</td>
</tr>
<tr>
<td>ldapcompare</td>
<td>ldapcompare is used to perform compare queries that print a message whether the result returned a match or not. ldapcompare opens a connection to an LDAP directory server, binds, and performs the comparison specified on the command line or from a specified file.</td>
</tr>
<tr>
<td>ldapconvert</td>
<td>ldapconvert is a utility program to port from Member mode to MemberOf mode. This is done by searching all specified group/template entries and fetching their Member attribute values. Each value is the DN of a member entry. The entry identified by this DN will be added to the MemberOf attribute value of the group/template DN at hand. In addition, those Member attribute values will be deleted from the group/template unless Both mode is specified. While running the program, a log file named ldapconvert.log is generated in the current directory, logging all modifications done and errors encountered.</td>
</tr>
<tr>
<td>ldapmodify</td>
<td>ldapmodify imports users to an LDAP server. The input file must be in the LDIF format.</td>
</tr>
<tr>
<td>ldapsearch</td>
<td>ldapsearch queries an LDAP directory and returns the results.</td>
</tr>
<tr>
<td>log_export</td>
<td>log_export is a utility that allows you to transfer Log data to an external database. This utility behaves as a LEA client. LEA (Log Export API) enables Security Gateway log data to be exported to third-party applications. log_export receives the Logs from the Security Management server via LEA so it can be run from any host that has a SIC connection with the Security Management server and is defined as an OPSEC host. log_export should be defined as a reporting Security Gateway in order to act in a distributed environment. To run log_export, you need a basic understanding and a working knowledge of: - Oracle database administration - LEA</td>
</tr>
<tr>
<td>queryDB_util</td>
<td>queryDB_util enables searching the object database according to search parameters.</td>
</tr>
<tr>
<td>rs_db_tool</td>
<td>rs_db_tool is used to manage DAIP Modules in a DAIP database.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sam_alert</td>
<td>This tool executes Check Point SAM (Suspicious Activity Monitoring) actions according to information received through Standard input. This tool is for executing SAM actions with the Check Point User Defined alerts mechanism.</td>
</tr>
</tbody>
</table>
Index

A
A Typical Object Configuration • 15
Account Units • 116
Account Units and High Availability • 117
Active versus Standby • 148
Actualizing an Implied network • 42
Add a Connectivity Cloud • 42
Add a Network Object to SmartMap • 40
Add an Internet Cloud • 42
Add License Details Manually • 112
Adding a Policy to an Existing Policy Package • 35
Adding a Section Title • 35
Adding New Attributes to the Active Directory • 129
Adding New Licenses to the License & Contract Repository • 111
Adding New Packages to the Package Repository • 106
Adding the contents of a SmartMap folder to the Rule Base • 44
Address Ranges • 169
Adjusting and Customizing SmartMap • 39
Adjusting SmartMap using the Navigator • 39
Advanced Search Attributes • 55
Advanced Tracking Operations • 74
Affecting SmartMap Layout (Arranging Styles) • 39
Anti-spoofing Parameters and OSE Devices Setup (Cisco and Nortel) • 167
Assigning and Removing Group Membership • 18
Attaching Licenses • 112
Attributes • 131
AttributesTranslationMap • 141
Authenticating the Administrator • 12
Authenticating the Security Management Server Using its Fingerprint • 12
Authenticating with the SmartDirectory (LDAP) Server using Certificates • 126
AutomaticAttrs • 145

B
Backing Up the Security Management server • 147
Backup and Restore the Security Management server • 97
BadPwdCountAttr • 140
Balance Method • 168
Basic Search Attributes • 55
Basic Tracking Configuration • 75
Block Intruder • 85
Blocking Intruders • 74
BranchObjectClass • 141
BranchOCOOperator • 141

C
CA Cleanup • 58
CA Data Types • 59
Calculating topology information • 45
Canceling an Operation • 108
Certificate Longevity and Statuses • 49
Certificate Operations Using the ICA Management Tool • 56
Changing a Column's Width • 80
Changing the Active SMS to the Standby SMS • 153
Changing the Standby SMS to the Active SMS • 153
Changing the Status of the Security Management server • 150
Changing the View in the Objects Tree • 15
Check Connectivity • 93
Check Domain Administrator Credentials • 93
Check Point Advisory • 74
Check Point CD • 106
Check Point Host • 164
Check Point Objects • 164
Check Point Schema • 119
Checking for Expired Licenses • 113
Choosing the Appropriate Tracking Option • 75
Choosing which Rules to Track • 74
Classic View of the Objects Tree • 16
Clearing the Repository of Completed Operations • 105
CLI Appendix • 170
Client Side Requirements • 100
ClientSideCrypt • 140
cn • 132
Collapsing locales • 43
Collapsing other Topology Structures • 43
Common Operations • 104
Completing Configuration • 91
Configuration • 89
Configure Automatic Deletion • 96
Configuring a Filter • 77
Configuring a New Query • 35
Configuring Administrators • 26
Configuring Advanced Settings • 91
Configuring Alert Commands • 85
Configuring Groups • 27
Configuring Identity Logging • 89
Configuring Objects • 15
Configuring Queries • 78
Configuring Security Gateways for SNMP • 158
Configuring Security Gateways for SNMP Requests • 158
Configuring Security Gateways for SNMP Traps • 159
Configuring SmartDirectory (LDAP) Entities • 121
Configuring Templates • 26
Configuring the CA • 59
Configuring the Current Rule Number Filter • 77
Configuring the Firewall • 89
Configuring User Objects • 25
Configuring Users • 25
Connecting a network to Connectivity clouds/an Internet cloud, where there is more than one/a Containing Network • 42
Connecting a Network to Internet Clouds • 42
Connecting multiple networks to a Connectivity Cloud • 42
Connecting to the Management Portal • 101
To Install a Policy Package • 28
To modify a predefined Query and save it under a new name • 79
To save the changes made to a custom Query • 79
To select the level of magnification • 39
To Uninstall a Policy Package • 28
Toggle SmartMap • 39
Tour of SmartDashboard • 13
Tracking Configuration • 75
Tracking Considerations • 74
Tracking Management High Availability Throughout the System • 155
Tracking Network Traffic • 64
Tracking Overview • 64
Transferring Files to Remote Devices • 107
Troubleshooting • 92
Troubleshooting duplicated networks • 46
Troubleshooting SIC • 22
Troubleshooting Tools • 101
Troubleshooting unresolved object interfaces • 46
Troubleshooting with SmartMap • 45

U
uid • 133
Understanding SIC Trust States • 22
Understanding SmartUpdate • 103
Understanding the Rule Color Legend • 45
Understanding the SNMP MIB • 157
Uninstalling Distributions and Upgrades • 108
Updating a Single Package on a Check Point Remote Gateway • 107
Updating the registry settings • 129
Upgrading All Packages on a Check Point Remote Gateway • 107
Upgrading Packages • 105
Upgrading UTM-1 Edge Firmware with SmartUpdate • 108
Use wbemtest to Verify WMI • 92
User and Administrator Types • 25
User Center • 106
User Certificate Management • 50
User Management Requirements • 24
UserLoginAttr • 138
UserMembershipAttr • 143
UserObjectClass • 142, 145
UserOCOperator • 142
userPassword • 133
UserPasswordAttr • 139
UserRDN • 144
Users Database • 24
UserTemplateMembershipAttr • 144
Using a Dynamic IP Address • 161
Using a Simple Non-LDAP Query • 58
Using an LDAP Query • 57
Using SmartDirectory (LDAP) Queries • 126
Using the Management Portal • 101
UTM-1 Edge Gateway • 164

V
Verify the WMI Service • 93
Verifying the Viability of a Distribution • 107
Version Configuration • 96
Version Diagnostics • 97
Version Operations • 95
Version Upgrade • 97
View a Version • 95
Viewing a Network Object selected in the Rule Base in SmartMap • 44
Viewing a Record's Details • 81
Viewing a Rule • 81
Viewing and Managing Objects • 163
Viewing and Saving Certificate Details • 56
Viewing Gateway Clusters • 44
Viewing License Properties • 113
Viewing Network Objects selected in SmartMap in the Rule Base • 45
Viewing Operation Details • 105
Viewing Packet Capture • 74
Viewing the Content of • 43
Viewing the Logs of a Rule from SmartDashboard • 72
Viewing the Logs of a Rule from the Rule Base • 78
Viewing the Matching Rule in Context • 72
Viewing the Settings of an Implied network • 42
VoIP Domains • 169

W
What Data is Backed Up by the Standby Security Management servers? • 149
What is SmartMap Helper? • 46
What objects can be defined as protected objects? • 46
When Synchronization Fails • 151
Working with Folders in SmartMap • 43
Working with Log Servers • 83
Working with Multiple SmartDirectory (LDAP) Servers • 119
Working with Network Objects and Groups in SmartMap • 40
Working with Policies • 27
Working with SmartDirectory (LDAP) for CRL Retrieval • 124
Working with SmartDirectory (LDAP) for User Management • 123
Working with SmartMap • 38
Working with SmartMap Objects • 41
Working with SmartMap Output • 47
Working with SNMP Management Tools • 156
Working with the Query Properties Pane • 80
Working with the SmartDirectory (LDAP) Profile • 121