Software Blades R7x

CC Evaluated Configuration
Administration Guide

March 2012
# The Common Criteria Evaluated Configuration

## CHAPTER 1  Overview
- The Certification Challenge ............................................... 11
- Reference Material ............................................................. 13
- How to use this Administration Guide ............................... 13

## CHAPTER 2  Physical Boundaries
- Components of the Evaluated Configuration ..................... 16
- Security Management server .............................................. 16
- SmartConsole (Management GUI) ..................................... 17

## CHAPTER 3  Administration Interfaces
- Management Functionality ................................................ 20
- SmartConsole ................................................................. 22
  - SmartDashboard ....................................................... 22
  - SmartView Tracker .................................................. 23
  - SmartView Monitor .................................................. 23
- Administrator Access Control ........................................... 23
- Permissions Profiles ....................................................... 24
- Administrator Accounts .................................................. 25

# Security Policy

## CHAPTER 4  Creating the Security Policy
- Overview ............................................................................ 30
  - Security Policy Considerations ........................................ 30
  - Defining Basic Objects .................................................. 30
  - Cluster Considerations .................................................. 31
  - Defining Management Objects ................................. 31
 CHAPTER 6  IPS Settings  88
  IPS Console ................................................................. 88
  IPS Gateway Object Settings ........................................ 90

 CHAPTER 7  Site to Site VPNs  92
  Defining a Trusted CA .................................................. 93
  Defining an LDAP Account Unit ..................................... 94
  IPSec VPN Configuration between Managed Gateways ... 96
  VPN Configuration with Externally Managed Gateways .. 98
  Configuring VPN Communities ..................................... 98
  Defining VPN in Global Properties ............................... 106
  Implied Rules and VPN ................................................ 109
  Wire Mode .................................................................... 110

 CHAPTER 8  Remote Access VPN  112
  User Configuration ....................................................... 113
    Users ........................................................................ 113
    User Groups ................................................................ 114
  Configuring Remote Access in the Gateway Object........ 115
  Configuring the Remote Access Community .................. 119
  Configuring Remote Access in Global Properties .......... 122
  Defining Remote Access Rules ...................................... 130

 CHAPTER 9  Content Inspection Settings  132

 CHAPTER 10  Security Policy Installation  134
  SIC Trust Establishment ............................................... 134
    Obtaining the Activation Key ....................................... 135
    Trust Establishment .................................................. 137
  Security Policy Installation ........................................... 139

 Monitoring  140

 CHAPTER 11  Monitoring System Status  142
  SmartView Monitor ....................................................... 142
    Overview .................................................................... 142
CHAPTER 12  Monitoring Traffic  148

Alerts  144
Status Displays  145
Gateway Information  146

APPENDIX A  Management Functions  154

Security Policy installation and policy revision control... 155
Management of multiple authentication mechanisms ..... 155
Management of audit generation settings .................... 158
Control of communication with external IT entities ..... 158
Modification of IPS System behavior ......................... 160
Enabling or disabling Security Policy implied rules .... 161
Enabling SIC connectivity ........................................ 161
Management of Rule Base and VPN Communities ...... 162
User management .................................................. 163
Object database management .................................. 163
Audit trail management ......................................... 163
Exporting log records to a file ................................ 164
Performing audit queries ....................................... 164
Defining monitoring thresholds for resource values .... 165
Monitoring resource levels and connectivity status ...... 165
Viewing alerts ..................................................... 165
Fault Tolerance .................................................... 166
The Common Criteria Evaluated Configuration
CHAPTER 1

Overview

In This Chapter

The Certification Challenge page 11
Reference Material page 13
How to use this Administration Guide page 13

The Certification Challenge

"Common Criteria for Information Technology Security Evaluation" (CCITSE) usually referred to as the "Common Criteria" (CC) is an evaluation standard for a multi-national marketplace. The uses of Common Criteria include:

- For consumers:
  - To find requirements for security features that match their own risk assessment.
  - To shop for products that have ratings with those features.
  - To publish their security requirements so that vendors can design products that meet them.

- For developers:
  - To select security requirements that they wish to include in their products.
  - To design and build a product in a way that can prove to evaluators that the product meets requirements.
To determine their responsibilities in supporting and evaluating their product.

This document describes the operation procedures that must be implemented by Check Point Software Technologies Ltd. customers and/or resellers for the configuration and management of Check Point Software Blades R7x in accordance with the Common Criteria evaluated configuration, as defined in the Check Point Software Blades R7x Security Target.

The document also describes the administrative security functions and interfaces available to the administrator of the evaluated configuration. It identifies and describes the purpose, behavior, and interrelationships of the administrator security interfaces and functions.

The guidelines given in this document are most often exceptions or constraints to the instructions written in the referenced documentation. If a feature or service is listed below, you must configure the mentioned item as described here. If a feature or service is not listed below, configure it as written in the referenced documentation.

If you follow the requirements in this document when setting up and using the system, your configuration will match the evaluated configuration.
Reference Material

The evaluated configuration is described in:

- *Check Point Software Blades R7x Security Target*

Installation guidance is provided in:

- *CC Evaluated Configuration Installation Guide Version R7x*

See the following Check Point administration guides provided on the product CD-ROMs for more information on Check Point Software Blades R7x administration:

- *Security Management Server R71*
- *SmartView Monitor R71*
- *IPS R71*
- *Firewall R70*
- *Virtual Private Networks Version R70*
- *ClusterXL R70.1*

How to use this Administration Guide

The first three chapters provide an overview of the evaluated configuration and of its security management functionality.

*CHAPTER 4 Creating the Security Policy* provides step by step instructions for setting up a basic Security Policy that can be installed on Security Gateway in the evaluated configuration. These instructions *must* be followed completely to ensure that all parameter values are set in their secure values.

Use these instructions in conjunction with the instructions given in the *CC Evaluated Configuration Installation Guide Version R7x* to ensure that the product is initially installed in its evaluated configuration; thereafter, use this Administration Guide to ensure that all administration settings remain in their secure values.
The next four chapters provide additional instructions that are to be applied if the following functionality is required: Security Servers, IPS, Site to Site VPNs, and Remote Access VPNs, respectively. The step by step instructions provided by these chapters are also mandatory in these scenarios; they are broken down into separate chapters to allow for scenarios that do not require such functionality.

CHAPTER 9 Content Inspection Settings instructs the administrator to disable automatic updates for content inspection functionality, which is outside the evaluated configuration.


CHAPTER 11 Monitoring System Status describes the use of the SmartView Monitor application for monitoring system status. CHAPTER 12 Monitoring Traffic describes the use of the SmartView Tracker application for reviewing and managing logs and audit records.
CHAPTER 2

Physical Boundaries

In This Chapter

Components of the Evaluated Configuration page 16
Security Management server page 16
SmartConsole (Management GUI) page 17
Components of the Evaluated Configuration

The evaluated configuration includes the following components:

- **Security Gateway** - Check Point Software Blades R7x software installed on an appliance running the Check Point SecurePlatform operating system.
- **Security Management Server** - management server software installed on a host running the Check Point SecurePlatform operating system.
- **SmartConsole** – management GUI software installed on a host running a Microsoft Windows operating system. The SmartConsole hardware and operating system are not considered part of the evaluated system – they are installed and configured by the administrator as needed to support the Check Point application.
- **SSL Network Extender** and **SecureClient Mobile** – SSL VPN clients that can be downloaded from the Security Gateway to the user's workstation.

An evaluated configuration includes one or more Security Management servers, one or more Security Gateways, and one or more SmartConsoles. (Fault tolerant configurations require two or more of each component).

Security Management server

The Check Point Software Blades R7x media includes management server software, Security Management server. A Security Management server manages one or more Check Point Software Blades R7x appliances. It is used to perform management operations, to monitor the evaluated configuration's correct operation and to provide administrators with search and sort capabilities on the audit trail and IDS System data.

The evaluated configuration supports both local and remote management through the Security Management server. Management interfaces include the SmartConsole management GUIs (SmartDashboard, SmartView Tracker and SmartView Monitor).
SmartConsole (Management GUI)

The evaluated configuration includes three SmartConsole management GUI applications that are included on the Check Point Software Blades R7x media: SmartDashboard, SmartView Tracker and SmartView Monitor. These applications are installed on standard PC administrator workstations running Microsoft Windows, and are used as the only management interface for the operational evaluated configuration. The management GUI applications interact with the Security Management server.

These GUI applications allow an authorized administrator to manage the evaluated configuration rule base and general configuration, monitor its status, and review audit trail and IDS System data.

**Note:** The CLI and database editing tool are *not* to be used after installation and generation of the evaluated configuration. After installation is complete, do *not* log in to the Security Management server or Security Gateway consoles. SmartConsole certificate-based login should be used exclusively.

It is recommended that administrators should *not* be provided console login and cpconfig administrator passwords.
CHAPTER 3

Administration Interfaces

In This Chapter

Management Functionality  page 20
SmartConsole  page 22
Administrator Access Control  page 23
Permissions Profiles  page 24
Administrator Accounts  page 25
Management Functionality

The evaluated configuration’s primary functionality is to mediate information flows between controlled networks. The evaluated configuration mediates the information flows according to an administrator defined policy.

The evaluated configuration can be configured by an authorized administrator to require user authentication before allowing a given information flow. The product supports a number of authentication methods, including certificate-based authentication (requiring an IKE/IPSec remote access VPN connection for a given information flow), IKE shared-secret authentication, multiple-use passwords stored on the Check Point Software Blades R7x appliance, as well as authentication using an external server in the IT environment.

In the evaluated configuration, the administrator configures a single-use authentication mechanism (implemented using IKE, RADIUS or SecurID) for Telnet and FTP (if these services are allowed), as a condition for compliance with the Application-level Firewall Protection Profile. Specify in SmartDashboard, for any rule that allows the protocols FTP or Telnet, one of the following (it is not possible to specify both): either User Auth in the Action column of the rule base, or a remote access VPN in the VPN column.

A Check Point Software Blades R7x appliance can be configured by an authorized administrator to establish an IPSec VPN tunnel with a remote peer IT entity. Management of VPN rules is performed by associating VPN peers with a VPN community defined by the administrator.

The authorized administrator can configure the evaluated configuration to generate alerts for selected events. Alerts can be displayed in a pop-up window on the SmartConsole, or be sent out as SNMP traps.
Authorized administrators manage the evaluated configuration and review audit trail and IDS System data via the Security Management server and SmartConsole GUI. Audit trail data is stamped with a dependable date and time when recorded.

Auditable events include:
- modifications to the group of users associated with the authorized administrator role
- all use of the identification and authentication mechanisms (including any attempted reuse of authentication data)
- all information flow control decisions made by the evaluated configuration according to the security policy rules
- the use of all security functions

If the audit trail becomes filled, then the only auditable events that may be performed are those performed by the authorized administrator. The evaluated configuration includes tools to perform searching and sorting on the collected audit trail data according to attributes of the data recorded and ranges of some of those attributes.
SmartConsole

SmartDashboard

SmartDashboard lets the administrator view and modify object attributes. Objects are created by the system administrator in order to represent actual hosts and devices, as well as logical 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.

The abstract Security Policy is translated by the Security Management server into information flow control rules as well as global and local policy settings that may be installed by the administrator, using the SmartDashboard GUI, on one or more Check Point Software Blades R7x appliances.

The following security-relevant management functions are provided to the authorized administrator via the SmartDashboard Management GUI. They include:

- Security Policy installation and policy revision control
- user management
- management of multiple authentication mechanisms
- control of communication with external IT entities
- management of audit generation settings
- enabling SIC connectivity
- enabling or disabling Security Policy implied rules
- Management of Rule Base and VPN Communities
- modification of IDS System behavior
- Object database management
**SmartView Tracker**

The SmartView Tracker Management GUI provides the authorized administrator and the authorized audit administrator with the capability to perform audit queries.

The following security-relevant management functions are provided to the authorized administrator via the SmartView Tracker Management GUI. They include:
- audit trail management
- exporting log records to a file
- performing audit queries

**SmartView Monitor**

The following security-relevant management functions are provided to the authorized administrator via the SmartView Monitor Management GUI. They include:
- defining monitoring thresholds for resource values (CPU, disk, etc.)
- monitoring resource levels and connectivity status
- viewing alerts

**Administrator Access Control**

The Security Management server maintains a user database. The user database is distributed to the evaluated configuration’s Check Point Software Blades R7x appliances. The user database contains entries for both administrators and other users of the evaluated configuration.

For each user, the user database stores the following security-relevant attributes:
- user identification
- association with an administrator permissions profile
- one-time password authentication method, IKE shared-secret or certificate (administrators use only certificate-based authentication in the evaluated configuration); and
- group memberships (if any).
When creating an administrator entry in the user database, the user must be associated with a permission profile. There are four high-level permission classes:

- **None**: Restricts the user from accessing any of the SmartConsole Management GUIs.
- **Read/Write All**: Allows full access (Read/Write) to all three SmartConsole Management GUIs. An additional modifier, Manage Administrators, is required for an administrator to be able to manage administrator user attributes.
- **Read Only All**: Allows the administrator to access all three SmartConsole Management GUIs with all permissions set to Read Only, restricting him or her from performing any modifications to the evaluated configuration or to evaluated configuration data.
- **Customized**: Provides more granular control over administrator restrictions. The Manage Administrators permission is only available for Read/Write All.

The Security Management server restricts all management functions according to the user's permission profile.

**Permissions Profiles**

Two default permissions profiles are configured in the evaluated configuration: AuthorizedAdministrator and AuditAdministrator (see First Time Login in the *CC Evaluated Configuration Installation Guide*).

The AuthorizedAdministrator permissions profile is assigned Read/Write All with Manage Administrators. The AuditAdministrator permissions profile is a Customized permissions profile assigned the Objects Database, Check Point Users Database, Monitoring, Track Logs, and Audit Logs permissions, all in Read Only mode.

Administrators that are associated with the AuthorizedAdministrator permissions profile are authorized to perform all SmartConsole management functions. Administrators that are associated with the
AuditAdministrator permissions profile are restricted to the SmartView Tracker and SmartView Monitor applications; they cannot log in to the SmartDashboard. In addition, they are prevented from performing log management operations (log switch, log purge, log export, remote file operations), modifying monitoring thresholds, and any other management operations apart from viewing logs, alerts, and system status.

Permission profiles that contain a subset of the permissions of the authorized administrator role but are not the authorized audit administrator role may also be defined.

**Note:** Read/Write access to SmartDashboard allows the administrator to define scripts that are executed (with root privileges) on the Security Management server or on Security Gateway in certain situations, e.g. when an alert is generated, or when old log files are deleted. These settings should not be used, as they can result in arbitrary results that may cause a violation of the evaluated configuration security policy.

**Administrator Accounts**

When creating an administrator account, you must generate and save a certificate to be used by the new administrator. The certificate should be saved to offline media and securely delivered to the administrator, together with the password used to protect it. Make sure that no one but the intended administrator can gain access to the certificate file, either during delivery or post-delivery.

If there is any reason to suspect that the administrator has lost sole control over his or her certificate file, revoke the certificate immediately and generate a new one for the administrator.

Administrators may only use single-use authentication schemes. Verify that the **Authentication Scheme** is **Undefined**, **RADIUS**, or **SecurID** in the **Authentication** tab of the **Administrator Properties** window before saving a new or modified administrator object.
Security Policy
CHAPTER 4

Creating the Security Policy

In This Chapter

Overview page 30
Defining Management Objects page 31
Creating the Security Cluster or Gateway Objects page 36
Defining Global Properties page 50
Defining Rules page 58
Creating a Policy Package page 58
Management Rules page 59
Overview

Security Policy Considerations

When planning your Security Policy a number of issues must be taken into consideration. These include:

- Which services are allowed across the network
- User permissions and authentication schemes needed
- Objects in network (clusters, gateways, networks, routers, domains)

Security Policy creation entails the following steps:

- Defining Management Objects
- Defining Cluster and Gateway Objects
- Defining Global Properties
- Creating a Policy Package
- Defining Rules
- Installing the Policy

The default security policy is restrictive – it does not allow any information flows through the Security Gateway. A Security Policy must be installed in order to enable any information flow. The instructions in this chapter must be followed when defining and installing a Security Policy; a partial or divergent Security Policy might contain exploitable vulnerabilities, or might cause communication failures between the Security Management server and Security Gateway, requiring reinstallation.

Defining Basic Objects

Objects are created by the system administrator in order to represent actual hosts and devices, as well as logical 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.

Follow the instructions provided in Configuring Objects, in Chapter 1 of the *Check Point Security Management Server R71 Administration Guide* to define Basic Objects.

In the evaluated configuration, you will be defining various objects, including: a primary Management Module and a secondary Management (if implementing Management High Availability), at least one Security Gateway, machines that run various Servers that are defined as part of the system, or from which the system requests services, resources, users and VPN communities.

**Cluster Considerations**

A Security Gateway may be either installed individually or as a cluster member. A cluster of two or more gateways behaves as a redundant gateway. Its configuration is equivalent to that of an individual gateway. Cluster object configuration settings are replicated to each member gateway object. In the following subsections, required configuration settings are shown for an individual gateway but should be applied to cluster objects in the same way, when using a cluster configuration.

**Defining Management Objects**

**Configuring the Primary Management Object**

1. From the Objects Tree in SmartDashboard, expand the *Check Point* branch and double-click the Management Server object name. (The Management Object is created automatically.) Alternatively, you can select *Network Objects* from the Manage menu: the *Network Objects* window appears; select the Management Server object name, and click *Edit*....
2. Configure the **General Properties** page:

Set only the **Logging & Status** software blade check box under the **Management** pane (some check boxes, e.g. Network Policy Management, will be automatically set by the product installation process). The **Monitoring** software blade may also be optionally selected.

**Note:** The following software blades are *not* included in the evaluated configuration: Endpoint Policy Management, Management Portal, Workflow, User Directory, SmartReporter, SmartEvent, SmartEvent Intro.
3. Configure the **Logs and Masters** page:

![Logs and Masters Configuration Interface]

**Notes:** In the evaluated configuration, there is no direct administrator interface for manually deleting or purging log files on the Security Management server. These files accumulate both from audit files generated by the Security Management server, and from log files forwarded by the Security Gateway.

The settings on the **Logs and Masters** page for the Management Object allow the administrator to control the amount of disk storage taken up for log file storage as follows:

- **Required Free Disk Space** – by setting a value for this attribute, the administrator ensures that the defined amount (or
percentage of total disk space) is freed up by deleting old log files.

- **Do not delete log files from the last _ days** – this setting allows the administrator to protect recent log files from deletion when using the Required Free Disk Space feature.

- **Advanced…** - this control allows the administrator to define an arbitrary script that runs before log files are deleted, e.g. for writing the files to removable storage. This control should *not* be used in the evaluated configuration.

- **Alert when free disk space is below _** - set this control so that an alarm is sent when Security Management server disk resources are running out. When such an alarm is generated, you can back up old log files (using the Export… command in SmartView Tracker), and use the Required Free Disk Space setting to free up disk space on the Security Management server.

- **Stop logging when free disk space is below _** - this control must *not* be used in the evaluated configuration – it stops log record forwarding from Security Gateway when free disk space on the Security Management server is below an administrator-defined value. The log records will still be accumulated on the Security Gateway; however, the online review of audit records in SmartView Tracker and the review of Alerts in SmartView Monitor will be effectively disabled.

**Note:** In the evaluated configuration, the administrator is required to set a value for Alert when free disk space is below _. 
4. In the **Identity Logging** page:

   - Do *not* set **Enable display of user and computer names based on Active Directory mappings**.

![Identity Logging Page](image-url)
Configuring the Secondary Management Object

Chapter 11 of the Security Management Server R71 Administration Guide explains how to set up Management High Availability. Follow the steps described in Chapter 11 section Secondary Management Creation and Synchronization – the First Time to initialize the secondary management host. This process copies the configuration of the primary management server, so no additional evaluated configuration settings are required.

Creating the Security Cluster or Gateway Objects

This section describes the definition of the security gateway or cluster object, including all secure values that need to be set for this object. Once defined, the object can be used in Security Policy rules.

To define the gateway or cluster object, perform the following steps:

1. From the Objects Tree in SmartDashboard, right click Network Objects and select New > Security Gateway… if configuring an individual gateway, or New > Security Cluster… if configuring a cluster object.
2. Select the Classic mode. The Check Point Gateway General Properties page is displayed.

In order for the Security Policy to be installed on the gateway, secure communication must be established to the gateway using the Communication… button on the gateway object’s General Properties page; this process is performed after the gateway object has been defined, and is described in CHAPTER 10 - Security Policy Installation.
3. Configure the **General Properties** page:

Set only the **Firewall**, **IPSec VPN**, and **IPS** check boxes under Network Security pane. If configuring a cluster object, also set the **ClusterXL** check box (appears under the Acceleration & Clustering heading).

**Note:** In the evaluated configuration, the Security Gateway Object should *not* be defined as running any application other than those listed above.

**Note:** The SSL VPN software blade (not supported in the evaluated configuration) isn’t needed for supporting SSL Network Extender functionality included in the evaluated configuration.
Cluster Object Configuration

When using a cluster configuration, follow the instructions in this subsection to create the cluster and gateway objects. The next section explains how to create a non-clustered gateway object.

4. On the Cluster Members page, click Add > New Cluster Member and configure each cluster member’s name and IP address.

5. In the ClusterXL page:

- Do not set High Availability - Legacy mode.
6. In the **Topology** page for the cluster object, click **Edit Topology**:

- Configure the topology for each member interface.
- In the **Network Objective** column, do **not** use combined Cluster and Sync interfaces (e.g. ‘Cluster + 1st Sync’), as Synchronization interfaces must be assigned to dedicated, secured interfaces that are not accessible by any internal or external network.
- It is recommended to assign redundant Sync interfaces, in order to ensure continued operation in case of interface failure.
Non-Clustered Gateway Object Configuration

When using a non-clustered configuration, define the gateway topology as follows:

4. Open the gateway object created above in step 1.
5. Configure the **Topology** page for the gateway:

- Configure the relevant interfaces.
6. For each interface:
   a. Select the interface, click **Edit**. The **Topology** tab of the **Interface Properties** window is displayed.

   ![Interface Properties Window]

   b. Select **External** for external interfaces and **Internal** for internal interfaces (that have known sets of valid addresses).

   c. Select **Network defined by the interface IP and Net Mask** or defines **Specific** network objects that restrict the range of valid addresses that may be located behind this interface.

   d. Set **Perform Anti-Spoofing based on interface topology** to ensure that anti-spoofing is performed for packets entering from this interface.

   e. Set ** Spoof Tracking** to **Log** or **Alert** if logging is desired for spoofed packets detected and dropped by the Security Gateway.
Common Configuration Settings

Follow the following steps for either cluster objects or non-clustered gateway objects:

7. In the **Logs and Masters** page:

- Do *not* set **Required Free Disk Space** on the Security Gateway; this setting may cause log files to be deleted before they are reviewed by the administrator.
- Set **Stop logging when free disk space is below** _ and **Reject all connections** to ensure that auditable events are prevented.
when there is insufficient disk space on the Security Gateway. When free disk space falls below the defined threshold, the module transitions into a fail-safe mode in which it no longer accepts any incoming or outgoing packets. This ensures that no audit records are lost in the event of storage exhaustion.

- **Alert when free disk space is below** _ – set this control so that an alarm is sent when Security Gateway disk resources are running out. When such an alarm is generated, verify that scheduled log forwarding is enabled to send log files to the Security Management server (see below). You can also use the SmartView Tracker **Remote Files Management...** command to fetch log files from the Security Gateway, freeing up local storage.
8. In the **Masters** page:
   - Click **Add...** to add the secondary management server as master, if implementing Management High Availability.
9. In the Log Servers page:

- Do not set **Use local definitions for Log Servers**.
- Click **Add...** to add the secondary management server as log server, if implementing Management High Availability.
- Verify that the **Always send logs to** setting for the Log Server (Security Management server) object includes both Logs and Alerts, as depicted above.
10. In the **Cooperative Enforcement** page:

- **Do not set** Authorize clients using Endpoint Security Server.
11. In the **Advanced** page (SNMP):

- Verify that SNMP is not configured.
12. In the **SAM** page:

- Do *not* set **Forward SAM clients' requests to other SAM servers**.
- Do *not* set **Use early versions compatibility mode**.
13. In the **Connection Persistence** page:

- It is recommended (although not required by the evaluated configuration) that **Rematch connections** be selected. If the administrator doesn't set **Rematch connections**, some connections may persist after a policy installation, even if those connections are not allowed by the new policy.

**Note:** When defining a Service Object, selecting the **Keep connections open after policy has been installed** checkbox overrides the settings in the **Connection Persistence** page.
Defining Global Properties

The Security Policy is made up of rules specified in the Security Rule Base. In addition to administrator-defined rules, Check Point Software Blades R7x also creates Implied Rules. These are defined in the Global Properties page.

Rule order is critical. Having the same rules, but placing them in a different order, can radically alter how your firewall works. It is therefore best to place the more specific rules first, the more general rules last. This prevents a general rule being matched before a more specific rule, and protects your firewall from misconfigurations. Implied rules may be placed first, last, or before last in the Security Rule Base.

This section describes settings that can be configured through selecting Policy > Global Properties in SmartDashboard.
14. In the **FireWall** page:

- Verify that **Accept control connections** is not selected.
- Verify that **Accept outgoing packets originating from Gateway** is not selected.
- Verify that **Accept SmartUpdate connections** is not selected.
15. In the Alert Commands page:

- If you wish to specify Alert Commands, only popup and SNMP trap alerts are considered part of the evaluated configuration. Do not use mail or user defined alerts.
If enabling SNMP alerts, you should replace 'localhost' with appropriate SNMP parameters, as follows:

```
[-v var] [-g generic_trap] [-s specific_trap] host [message]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v var</td>
<td>optional object ID to bind with message</td>
</tr>
<tr>
<td>-g generic_trap</td>
<td>one of the following values:</td>
</tr>
<tr>
<td></td>
<td>0 - coldStart</td>
</tr>
<tr>
<td></td>
<td>1 - warmStart</td>
</tr>
<tr>
<td></td>
<td>2 - linkDown</td>
</tr>
<tr>
<td></td>
<td>3 - linkUp</td>
</tr>
<tr>
<td></td>
<td>4 - authenticationFailure</td>
</tr>
<tr>
<td></td>
<td>5 - egpNeighborLoss</td>
</tr>
<tr>
<td></td>
<td>6 - enterpriseSpecific</td>
</tr>
<tr>
<td>-s specific_trap</td>
<td>unique number specifying trap type; valid only if generic_trap value is</td>
</tr>
<tr>
<td></td>
<td>enterpriseSpecific (default value is 0)</td>
</tr>
</tbody>
</table>

host          | name of host that should receive the trap                                |
message        | message sent to the host                                                  |
16. In the OPSEC page:

- Verify that **Allow remote registration of OPSEC products** is not configured.
17. In the SmartDashboard Customization > Advanced Configuration: select FireWall-1 > Web Security:

- Verify that `http_activate_ss_protections` is selected.
18. Select FireWall-1 > Security Servers > SMTP Security Server:

- Verify that `mdq_run_multi_threaded` is selected.
19. In Manage > Servers and OPSEC Applications… > internal_ca, select the **Local Security Management server** tab and clear HTTP Server(s):
**Defining Rules**

Follow the instructions in Access Control, in Chapter 1 of the *Check Point FireWall R70 Administration Guide* to define the rules required for access control.

The Security Policy is implemented by defining an ordered set of rules in the Security Rule Base. A well-defined Security Policy is essential in order for Check Point Software Blades R7x to be an effective security solution. The fundamental concept of the Security Rule Base is “That which is not explicitly permitted is prohibited”.

The Rule Base specifies what communication will be allowed to pass and what will be blocked. It specifies the source and destination of the communication, what services can be used, at what times, whether to log the connection, and the logging level.

**Creating a Policy Package**

A Policy Package is a set of Policies that are enforced by the Security Gateway. They can be installed or uninstalled together on selected Security Gateway.

Follow the instructions in Working with Policies, in Chapter 1 of the *Check Point Security Management Server R71 Administration Guide* to create a Policy Package.

**Warning:** Uninstalling the Policy Package from a Check Point Software Blades R7x appliance removes all Rule Base enforcement functionality; IP forwarding is disabled.
Management Rules

Since Accept control connections has been disabled, you must explicitly allow the following management rules in the Rule Base, to allow VPN-1 Security Gateway and the Security Management server to communicate with each other. Failure to completely define the rules described in this section could result in security functionality becoming unavailable. Define management rules in the order given in this section. See section Example for the Definition of Management Rules for an example of a default evaluated configuration Rule Base, showing these management rules.

The following Objects should be defined in the Objects Database for use in the proposed Rule Base.

- **GUI_clients** - Hosts on which SmartConsole clients are installed. This object will usually be defined as a Group or Network object.
- **Mgmt_server** – Security Management servers, including the primary management server, and if Management High Availability is used, all secondary management servers.
- **FireWalled_modules** – A group including all of the Security Gateway objects managed by the Security Management server(s).
- **Revocation_Repository** – LDAP or HTTP server for CRLs, or OCSP responder. Used for VPN configuration.
- **ThisModule** – This dynamic object is created on each appliance during installation according to the instructions in the Installation Guide. Create a new dynamic object in SmartDashboard – Manage > Network Objects… > New… Dynamic Object…, and name it “ThisModule” so it can be used in these rules.
- **ThisModule_All** – This dynamic object is create on each appliance during installation, and is equivalent to ThisModule on a non-clustered gateway. On a cluster member, it includes all member interface addresses, including both cluster and member addresses, and including all Sync interface addresses.
- **OPSEC_clients** – OPSEC clients using the LEA, ELA, or AMON protocols to connect to the Security Management server.
This section lists rules that should be defined to allow management traffic between Security Management server and appliances, between appliances and peer VPN gateways, and other control connections.

**Note:** The values for the VPN, TRACK and TIME columns in SmartDashboard should be set by the Administrator as needed. As described in Configuring VPN Communities, some of the management protocols (e.g. ICA_Push) have to be excluded from VPN communities so that the Security Management server can push new IPSec VPN Community rules to managed appliances. For these protocols, VPN column should be 'Any'. For the evaluated configuration, any values for the TRACK and TIME columns are acceptable.

**Note:** The Security Management servers are installed on a protected subnet that is directly connected to a Check Point Software Blades R7x appliance. The appliance protects the Security Management server from any network access by untrusted users. Do not allow any rules whose destination is the appliance or the Security Management server, other than those listed in this guidance document. Such rules have not been evaluated as part of the CC evaluated configuration. In particular, the Management Protection Rule (see below) is used to ensure that any rules specified by the administrator that have 'Any' as Destination do not apply to the management components.
Management Rules between the Security Management server and Appliances

The following rules must be defined by the Administrator in order to allow management traffic between the Security Management server and appliances:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt_server</td>
<td>FireWalled_modules</td>
<td>Any</td>
<td><strong>TCP</strong> CPD</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>TCP</strong> CPD_amon</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>TCP</strong> FW1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>TCP</strong> FW1_ica_push</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>TCP</strong> FW1_sam</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>TCP</strong> FW1_log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FireWalled_modules</td>
<td>Mgmt_server</td>
<td>Any</td>
<td><strong>TCP</strong> CPD</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>TCP</strong> FW1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>TCP</strong> FW1_log</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Management High Availability Rule

The following supports Management High Availability in configurations where the primary and secondary servers are separated by a gateway:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt_server</td>
<td>Mgmt_server</td>
<td>Any</td>
<td><strong>TCP</strong> CP_redundant</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
Remote Administration Rule

If Remote Administration (see *CC Evaluated Configuration Installation Guide Version R7x CHAPTER 3 - Deployment*) is to be configured, define the following Remote Administration rules, as appropriate:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI_clients</td>
<td>Mgmt_server</td>
<td>Any</td>
<td>CPMI</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>OPSEC_clients</td>
<td>Mgmt_server</td>
<td>Any</td>
<td>FW1_ela</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FW1_lea</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FW1_lea</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FW1_amon</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Management Protection Rule

The following rule protects the Security Management server and GUI machines from access by untrusted users (other than the rules listed above):

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Mgmt_server, GUI_clients</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
SNMP Alerts Rule

If SNMP Alerts are used, the following rule must be configured to allow SNMP traps to be sent from the Security Management server to the defined SNMP catcher:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt_server</td>
<td>catcher-host</td>
<td>Any</td>
<td>udp snmp-trap</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

NTP Rule

If NTP is used to synchronize clocks, the following rule must be configured to allow NTP requests to be sent from the Security Management server and gateways to the defined NTP servers:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt_server, ThisModule</td>
<td>NTP_Servers</td>
<td>Any</td>
<td>udp ntp-udp</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

IPS Updates Rules

If online IPS updates are to be supported, rules must be configured to allow outgoing http and https requests from the Security Management Server (scheduled updates) and from GUI clients (immediate updates):

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt_server, GUI_clients</td>
<td>Any</td>
<td>Any</td>
<td>tcp http tcp</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
**VPN Rules**

The following rules should be defined if VPN is configured:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThisModule</td>
<td>Any</td>
<td>Any</td>
<td><strong>UDP IKE</strong>&lt;br&gt;<strong>UDP IKE_NAT_TRAVERSAL</strong>&lt;br&gt;<strong>TCP IKE_tcp</strong></td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>Any</td>
<td>ThisModule</td>
<td>Any</td>
<td><strong>UDP IKE</strong>&lt;br&gt;<strong>UDP IKE_NAT_TRAVERSAL</strong>&lt;br&gt;<strong>TCP IKE_tcp</strong></td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>FireWalled_modules</td>
<td>FireWalled_modules</td>
<td>All_GwToGw</td>
<td><strong>UDP tunnel_test</strong></td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>Any</td>
<td>FireWalled_modules</td>
<td>RemoteAccess</td>
<td><strong>UDP tunnel_test</strong></td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

In addition, if certificates are being used for IKE authentication, a rule should allow revocation queries to applicable revocation repositories:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThisModule</td>
<td>Revocation_Repository</td>
<td>Any</td>
<td><strong>TCP http</strong>&lt;br&gt;<strong>TCP ldap</strong>&lt;br&gt;<strong>TCP ocsp</strong></td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

---

1 If desired, you may select only the features that are relevant to the specific VPN implementation, e.g. only IKE and not IKE_tcp, or allow tunnel_test only on All_GwToGw if remote access VPNs are not being used.
The following rule must be defined if MEP is configured:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>ThisModule</td>
<td>Any</td>
<td>UDP RDP</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

The following rule must be defined if SecureClient is configured:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>ThisModule</td>
<td>Any</td>
<td>TCP FW1_topo</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

**Note:** if **Support Visitor Mode** is enabled in the **Remote Access** page, an implied rule is automatically added to the Security Policy rule base, allowing incoming Visitor Mode traffic (default service: https) into the gateway.

The following rule should be installed on all gateways for which **Support L2TP** is enabled in the Remote Access page:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>ThisModule</td>
<td>Remote_Access_Community</td>
<td>UDP L2TP</td>
<td>Accept</td>
</tr>
</tbody>
</table>
Ping Rule

Consider adding a rule that allows outbound ICMP echo requests and IGMP from Security Gateways. In some clustered configurations, cluster members periodically perform connectivity tests using these protocols.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>FireWalled_modules</td>
<td>Any</td>
<td>Any</td>
<td>icmp-requests igmp</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
**Domain Separation Rule**

If the administrator defines a rule with 'Any' in the Destination column, this rule applies to Security Gateway as well. For example, a rule allowing http traffic to 'Any' will allow HTTP connections that terminate on the Security Gateway itself.

In order to ensure that no unintended connections are allowed into the Security Gateway, it is recommended to define the following rule. This rule will drop all traffic into Security Gateway that does not match the management and VPN rules defined above.

Note that this explicit rule overrides implied rules that are defined as 'Last' or 'Before Last' (unless it is the last rule in the Rule Base), but not implied rules that are defined as 'First'. For example, if **Policy > Global Properties… > Firewall > Accept ICMP requests** has been set and defined as 'First', Security Gateway will allow ICMP requests (e.g. 'ping' commands) to the module itself. If it has been defined as 'Last', ICMP requests will be allowed through the module, but not to the module.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>ThisModule_All</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

**Authentication Server Rules**

The following rule must be defined if RADIUS is used, to allow access from Security Management or Security Gateway to authorized RADIUS authentication servers.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt_server, ThisModule</td>
<td>RADIUS-Server</td>
<td>Any</td>
<td>UDP</td>
<td>RADIUS</td>
<td>Accept</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
The following rule must be defined if SecurID is used to allow access
from the Security Gateway to a directly connected SecurID server located
on a trusted subnet:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThisModule</td>
<td>SecurID_Server</td>
<td>Any</td>
<td>UDP SecurID_udp</td>
<td>Accept</td>
<td>&lt;gateway²&gt;</td>
</tr>
</tbody>
</table>

² SecurID servers are installed on protected subnets directly connected to the Security Gateway that require their services. If multiple SecurID servers are used in the evaluated configuration, the SecurID rule should be instantiated for each such protected subnet.
CVP and UFP Rules

The following rule must be defined if CVP is used:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThisModule</td>
<td>CVP_Server</td>
<td>Any</td>
<td>TCP FW1_cvp</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

The following rule must be defined if UFP is used:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThisModule</td>
<td>UFP_Server</td>
<td>Any</td>
<td>TCP FW1_ufp</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

Note: If a CVP/UFP server certificate is revoked, the administrator should install policy to the Security Gateway that were communicating with the CVP/UFP server, in order to ensure that a timely distribution of revocation information is being sent to those modules.
Example for the Definition of Management Rules

A sample basic rule base is depicted below. The management rules have been grouped under group headings to allow easy collapsing of these management rules. The administrator adds configuration-specific rules below these management rules.

This example depicts a configuration with VPN enabled and a RADIUS-based authentication server. In the example, SNMP Alerts and NTP requests have been allowed by the administrator to exit to 'Any'.

![Example Table and Diagram]
Configuring authenticated services may include the following procedures:

- Configuring Authentication in the Gateway Object
- User Configuration
- Authentication Server Configuration
- Security Servers Configuration
- Resource Definition
- OPSEC Server Definition
- Defining Security Server Rules
- Installing Policy
Configuring Authentication in the Gateway Object

1. From the Objects Tree in SmartDashboard, access the Authentication page of the Check Point Gateway Object.
2. In the Authentication page:

- In the Enabled Authentication Schemes area, verify that the Check Point Password, OS Password and TACACS checkboxes are unselected. (The evaluated configuration allows the use of the RADIUS and SecurID authentication schemes.)
- Set Authentication Failure Track as required. This setting determines whether failed user authentication attempts (when User
Auth has been specified for a given service) are logged and whether pop-up or SNMP alerts are generated as a result.

User Configuration

Authentication Rules are defined in terms of user groups, rather than in terms of individual users. You must therefore define users and add them to groups. You can define users using the proprietary user database. The user group cannot participate in Remote Access if it is not defined as being part of a Remote Access community.

Follow the instructions in Chapter 1 of the Check Point Security Management Server R71 Administration Guide and in Chapter 2 of the Check Point FireWall R70 Administration Guide to configure authentication.

Users

1. In the Users and Administrators tab, right click Users and select New User > Default... The User Properties window is displayed.
2. Alternatively, from the Manage menu, select Users and Administrators. The Users and Administrators window is displayed.
3. Click New and select User by Template > Default.... The User Properties window is displayed.
4. In the **Authentication** tab, select either **RADIUS** or **SecurID**. **Note:** In the evaluated configuration, **Undefined** may also be used as an authentication scheme, if remote access authentication is being used, or if the user doesn't need to access FTP or Telnet.
User Groups

1. From the Objects Tree in SmartDashboard, click the **Users and Administrators** tab.
2. Right click **User Groups** and select **New Group**. The **Group Properties** window is displayed.
3. Alternatively, from the **Manage** menu, select **Users and Administrators**. The **Users and Administrators** window is displayed.
4. Click **New** and select **User Group**. The **Group Properties** window is displayed.
5. Name the group and allocate defined users to the group.
Authentication Server Configuration

Configure the authentication servers from which the system requests authentication services.

RADIUS Server Definition

1. From the Objects Tree in SmartDashboard, click the Servers and OPSEC Applications tab.
2. Right click Servers and select New > RADIUS. The RADIUS Server Properties window is displayed.
3. Alternatively, from the Manage menu, select Servers and OPSEC Applications. The Servers and OPSEC Applications window is displayed.
4. Click New and select RADIUS. The RADIUS Server Properties window is displayed.

Note: The communication with the RADIUS server is protected using a MD5 Shared Secret. Secrets should be chosen out of a sufficiently large range (at least 16 random octets) in order to provide protection against exhaustive search attacks. It is also recommended to periodically change shared secrets.

ACE Server Definition

- Follow the instructions provided in the Configuring a VPN-1 Gateway to use SecureID section in the Check Point FireWall R70 Administration Guide.
Security Servers Configuration

Security Servers are proxy processes that must run on the evaluated configuration of Check Point Software Blades R7x. Security Servers are provided for the protocols: Telnet, FTP, HTTP and SMTP. When traffic that is associated with one of these protocols is received by the evaluated configuration, the traffic is redirected to be filtered by an appropriate Security Server. Security Servers validate access or service request for conformance to its associated published protocol specification. In addition, the evaluated configuration requires user authentication for the Telnet and FTP protocols.
Mail Security Server Configuration

1. In the IPS tab, select Mail Security Server, right click Mail Global Protection Scope and select See Details…
2. Select Default Protection > Edit…
3. Set Configurations apply to all connections.
FTP Security Server Configuration

1. In the IPS tab, select FTP right clicks FTP Security Server and select See Details…
2. Select Default Protection > Edit…
3. Set Configurations apply to all connections.
Resource Definition

Configure the resources utilized by the system, in conjunction with the Security Servers. Resources are mandatory for HTTP, and optional for the other security server protocols.

For HTTP
1. From the Objects Tree in SmartDashboard, click the Resources tab.
2. Right click Resources and select New > URI. The URI Resource Properties window is displayed.
3. Alternatively, from the Manage menu, select Resources. The Resources window is displayed.
4. Click New and select URI. The URI Resource Properties window is displayed.

- In the Use this resource to: area, verify that Enforce URI capabilities is selected.
- In the Connection Methods area, verify that Tunneling is not selected.
- In the Match tab, in the Schemes area, select http.
- In the CVP tab, verify that the CVP server is allowed to modify content checkbox is not selected.
For FTP
1. From the Objects Tree in SmartDashboard, click the Resources tab.
2. Right click Resources and select New > FTP. The FTP Resource Properties window is displayed.
3. Alternatively, from the Manage menu, select Resources. The Resources window is displayed.
4. Click New and select FTP. The FTP Resource Properties window is displayed.
5. Configure the FTP Resource Properties window.
6. In the CVP tab, verify that the CVP server is allowed to modify content checkbox is not selected
For SMTP

1. From the Objects Tree in SmartDashboard, click the Resources tab.
2. Right click Resources and select New > SMTP. The SMTP Resource Properties window is displayed.
3. Alternatively, from the Manage menu, select Resources. The Resources window is displayed.
4. Click New and select SMTP. The SMTP Resource Properties window is displayed.

- In the Mail Delivery area, select Check Rule Base with new destination checkbox.
- In the CVP tab, verify that the CVP server is allowed to modify content checkbox is not selected.
OPSEC Server Definition

If using CVP, UFP, or AMON, a OPSEC Server object must be defined for the CVP or UFP server. If using ELA or LEA, a OPSEC client object must be defined.

1. From the Manage menu, select Servers and OPSEC Applications. The Servers and OPSEC Applications window is displayed.
2. Click New and select OPSEC Application. The OPSEC Application Properties window is displayed.
3. In the Server Entities tab, you may select CVP, UFP, and AMON entity types, as required. In the Client Entities tab, you may select ELA and LEA entity types, as required. Do not select any of the other OPSEC application types.
CVP Options

1 In the OPSEC Application Properties window select the CVP Options tab.

2. Do not enable the Use early versions compatibility mode.
UFP Options

1. In OPSEC Application Properties window select UFP Options tab.

2. Do not enable Use early versions compatibility mode.
Defining Security Server Rules

Define Security server rules as required:

- All rules matching the Telnet protocol should be configured with an Action of ‘User Auth’.
- To ensure user authentication for FTP and Telnet traffic, configure either ‘User Auth’ as an Action, or specify a Remote Access VPN community in the VPN column of the rule.
- All HTTP rules must include a resource definition to ensure that the traffic is passed through a security server.

**WARNING**: If Any is specified in the Service field of an Accept rule, Telnet and FTP traffic may be matched to this rule, and be forwarded without authentication.
IPS Settings

IPS Console

The IPS console is divided into a tree structure that classifies the defenses provided by IPS.

Follow the instructions in Chapter 5 Configuring Specific Protections of the IPS R71 Administration Guide.

In the SmartDashboard toolbar, click the IPS tab.
In the Protections tab, select the IPS category to view information about the category. Most protections have graded parameters, provided to help you decide which protections to activate for security and which can be safely deactivated, for connectivity and performance. The protection parameters and their values for a specific protection appear at the top of the protection window.

Note: The supported products for each protection are listed under the description tab of the protection details.

Check the attacks you wish to defend against, and configure Settings for the categories and the specific attacks. Each protection has a mode, which
determines whether IPS inspects packets for this protection, and if so, what it does if the packet matches a threat symptom.

- **Inactive**: Packets are not inspected for this protection.
- **Prevent**: Packets are inspected and threatening packets or connections are dropped.
- **Detect**: Packets are inspected and threatening packets or events are tracked.

If the IPS policy settings cause a protection to be Inactive, and you want to activate it, select override with the action: and choose Prevent or Detect from the drop-down list.

You will need to reinstall the Security Policy in order to implement changes to the IPS configuration.

**Note:** Dshield Storm Center functionality is excluded from the evaluated configuration. The **Malicious IPs Protection** in all profiles setting must be maintained in **Inactive** mode (default).
IPS Gateway Object Settings

1. In the **IPS** page for the gateway or cluster object:

   - Do *not* set **Bypass IPS inspection when gateway is under heavy load**.
   - For the cluster object, select: **Prefer security – Close connections for which IPS inspection cannot be guaranteed**.
CHAPTER 7

Site to Site VPNs

In This Chapter

- Defining a Trusted CA  page 93
- Defining an LDAP Account Unit  page 94
- IPSec VPN Configuration between Managed Gateways  page 96
- VPN Configuration with Externally Managed Gateways  page 98
- Configuring VPN Communities  page 98
- Defining VPN in Global Properties  page 106
- Implied Rules and VPN  page 109
- Wire Mode  page 110
Defining a Trusted CA

1. From the Objects Tree in SmartDashboard, click the Servers and OPSEC Applications tab.
2. Right click Servers and select New > CA > Trusted. The Certificate Authority Properties window is displayed.
3. Alternatively, from the Manage menu, select Servers and OPSEC Applications. The Servers and OPSEC Applications window is displayed.
4. Click New and select CA > Trusted. The Certificate Authority Properties window is displayed.

![Certificate Authority Properties window]

5. In the OPSEC PKI tab, do not select the Automatically enroll certificate checkbox. Certificates will be loaded from a file.
6. Configure the Retrieve CRL From options based on your CA product and CRL distribution method.

Note: If CRLs are published on an LDAP server, verify that an account unit is defined for the directory.
Note: If OCSP validation has been configured for the CA object (see *CC Evaluated Configuration Installation Guide*), CRL settings will be ignored.

7. Configure CA properties according to your PKI product and get the CA certificate.

**Defining an LDAP Account Unit**

If your CA distributes CRL over LDAP, you will have to define an LDAP Account Unit object:

1. From the Objects Tree in SmartDashboard, click the **Servers and OPSEC Applications** tab.
2. Right click **Servers** and select **New > LDAP Account Unit**. The **LDAP Account Unit Properties** window is displayed.
3. Alternatively, from the **Manage** menu, select **Servers and OPSEC Applications**. The **Servers and OPSEC Applications** window is displayed.
4. Click **New** and select **LDAP Account Unit**. The **LDAP Account Unit Properties** window is displayed.
5. Verify that in the **Account Unit usage** area, the **CRL retrieval** checkbox is selected, and the **User Management** checkbox is *not* selected.

6. In the **Servers** tab, click **Add...** The **LDAP Server Properties** window is displayed.

7. Based on your LDAP Server settings, define the **Login DN** and **Password**, required to access CRL objects. If anonymous access is permitted, you may leave the field empty.

8. In the **Encryption** tab, based on your LDAP Server configuration, specify use of SSL, fingerprint and encryption strength.
IPSec VPN Configuration between Managed Gateways

From the Objects Tree in SmartDashboard, access the **IPSec VPN** page of the Check Point Gateway that is to participate in IPSec VPN.

If a VPN community in which this gateway participates is defined, it is listed in this area. VPN communities may be defined later.

**Note:** The gateway cannot participate in VPN or Remote Access if it is not defined as being a participating gateway of the appropriate community.
Although all Check Point Software Blades R7x gateways are automatically issued a VPN certificate by the Internal Certificate Authority (ICA), the evaluated configuration mandates the use of certificates that are issued by an external Trusted CA, other than the ICA. Follow the instructions in Configuration of PKI Operations, in Chapter 5 of the Virtual Private Networks R70 Administration Guide to generate a 3rd party certificate. The following procedure enforces the use of the 3rd party certificate for IKE tunnel establishment between managed gateways:

1. In the IPSec VPN page of the Security Gateway object, click Traditional Mode Configuration:

   ![Traditional mode IKE properties](image)

2. Select one or more of the following supported key exchange encryption algorithms: **3DES, AES-128, AES-256**.
3. **Do not** select MD5 as supported data integrity algorithm.
4. In the **Support authentication methods** area, select **Public Key Signatures**.


5. Click Specify. The **Allowed certificates** window is displayed.

![Allowed certificates window]

6. Specify the 3rd Party CA (in the example above, **kenny_ca**) and click OK.

### VPN Configuration with Externally Managed Gateways

The previous section describes the configuration of VPN between two internally managed gateways. You can also configure VPN with externally managed gateways. Follow the instructions in *Configuring a VPN with External Gateways Using PKI* or in *Configuring a VPN with External Gateways Using a Pre-Shared Secret* in Chapter 4 of the *Virtual Private Networks R70 Administration Guide* to configure VPN with externally managed gateways.

**Note:** If pre-shared secret keys are used for externally managed gateways, they should be generated using a cryptographically-strong (FIPS-approved) Random Number Generator (RNG).

### Configuring VPN Communities

This section describes settings that can be configured by selecting **Manage > VPN Communities**, or alternatively clicking the **IPSec VPN** tab of the Rule Base pane.

Edit existing Community or make a new Community. If you are configuring VPN for a Meshed Community:
1. In the **General** page:

- If **Accept all encrypted traffic** is not selected, you have to explicitly define the rules governing allowed services traffic between VPN peers.
2. In the **Participating Gateways** page:

- Add all gateways that are to participate in the VPN community.
3. In the **Encryption** page, you may select any of the presented options for **Encryption Method** and **Encryption Suite**:
4. If defining a **Custom** Encryption Suite (by clicking **Advanced**...):

- In the **IKE (Phase 1) Properties** area, verify that AES-128, AES-256 or 3DES have been selected in the **Perform key exchange encryption with** field.
- In the **IKE (Phase 1) Properties** area, verify that SHA1 or SHA256 have been selected for **Perform data integrity with**.
- In the **IKE (Phase 2) Properties** area, verify that AES-128, AES-256, or 3DES have been selected in the **Perform IPsec data encryption with** field.
- In the **IKE (Phase 2) Properties** area, verify that SHA1 or SHA256 have been selected for **Perform data integrity with**.
5. Configure the **Excluded Services** page:

This page selects services that are not tunneled over IPSec, even if they match VPN community rules. The administrator should consider excluding two types of services: services used for the establishment of the IPSec tunnel, i.e. are used before the tunnel has been fully established, and services that are used for control connections between Check Point products.

Control connections are protected using Check Point's Secure Internal Communications (SIC) facility, and therefore exclusion from the IPSec tunnel does not compromise security. In some configurations, VPN community definitions may interfere with these control connections.
- The following services are used to establish IPSec Tunnels:
  - RDP
  - IKE
  - IKE_NAT_TRAVERSAL
  - IKE_tcp

- The following services are used for control connections:
  - FW1
  - CPD_amon
  - CPD
  - FW1_ica_push
  - FW1_sam
  - FW1_log

See Management Rules in CHAPTER 4 for additional details on these management rules.
6. Configure the Advanced VPN Properties page:

In this page you can configure various elements relevant to the IKE negotiation or to the IPSec packets that pass between community members.
Defining VPN in Global Properties

1. Select **Global Properties** from the **Policy** menu and select the **VPN** page:

- Verify that **Simplified Mode** is selected.
2. In the VPN-Advanced page:

- Verify that Enable decrypt on accept… is not selected.
3. In the **Certificates** page:

- Verify that the **Renew users Internal CA Certificate** checkbox is not selected.
4. In the SmartDirectory [LDAP] page:

- Verify that **Use SmartDirectory (LDAP) for Security Gateways**... is not selected.
- Verify that **Use SmartDirectory (LDAP) for SSL VPN**... is not selected.

**Implied Rules and VPN**

Any Implied Rules that are applied as 'first' will be excluded from VPN community settings. Change this setting to 'before last' if IPSec is required for these services.
**Wire Mode**

Wire Mode, when configured on a gateway interface, allows all traffic exchanged over a Wire Mode-enabled VPN community to be received from or forwarded to the specified interface, without further Security Policy Rule Base inspection. The administrator may choose to log the traffic by setting **Log Wire mode traffic**.

---

**Warning**: Wire Mode, when enabled for an interface, will be applied for all Wire Mode-enabled VPN communities that include the gateway.
A Remote Access Community is a type of VPN Community. A user that belongs to a group in the community can establish a VPN with any Gateway defined for that community. A connection opened between the user's machine and a host in the VPN domain of the Gateway is encrypted.

In the evaluated configuration, the Remote Access VPN configuration procedure entails the following steps:

1. User Configuration to participate in Remote Access VPN
2. Configuring Remote Access in the Gateway Object
3. Configuring the Remote Access Community
4. Configuring Remote Access in Global Properties
5. Defining Remote Access Rules
6. Installing Policy
User Configuration

Authentication Rules are defined in terms of user groups, rather than in terms of individual users. You must therefore define users and add them to groups. You can define users using the proprietary user database. The user group cannot participate in Remote Access if it is not defined as being part of a Remote Access community.

Follow the instructions in Chapter 1 of the *Check Point Security Management Server R71 Administration Guide* and in Chapter 2 of the *Check Point FireWall R70 Administration Guide* to configure authentication.

Users

1. In the **Users and Administrators** tab, right click **Users** and select **New User > Default…** The **User Properties** window is displayed.
2. Alternatively, from the **Manage** menu, select **Users and Administrators**. The **Users and Administrators** window is displayed.
3. Click **New** and select **User by Template > Default….** The **User Properties** window is displayed.
4. To enable the user to participate in Remote Access VPN, verify that IKE is selected in the Client Encryption Method tab.

5. Follow the instructions in Configure Certificates Using Third Party PKI, in Chapter 14 of the Virtual Private Networks Administration Guide Version R70 to obtain certificates for users from 3rd party CAs. Also refer to Defining a Trusted CA and Defining an LDAP Account Unit in CHAPTER 7.

User Groups

1. From the Objects Tree in SmartDashboard, click the Users and Administrators tab.
2. Right click User Groups and select New Group. The Group Properties window is displayed.
3. Alternatively, from the Manage menu, select Users and Administrators. The Users and Administrators window is displayed.
5. Name the group and allocate defined users to the group.
Configuring Remote Access in the Gateway Object

1. Access the Remote Access page:

   - If Support L2TP is enabled do not use the MD5-Challenge as Authentication Method. Select a gateway certificate for Use this certificate.
   - Note: that Support Visitor Mode must be selected if SSL Network Extender or SecureClient Mobile functionality is required.
2. In the **Office Mode** page:

- Verify that the **Automatic (using DHCP)** radio button is not selected.
3. In the **Clientless VPN** page:

- Verify that the **Support Clientless VPN** checkbox is not selected.
4. In the VPN Clients page:

   - If SSL Network Extender or SecureClient Mobile functionality is to be used with this gateway, select the **SSL Network Extender** or **SecureClient Mobile** check boxes, respectively.
   - In **The gateway authenticates with this certificate** box, specify the certificate to be used by the gateway for SSL VPN.
   - Verify that the **Abra** checkbox is not selected.
Configuring the Remote Access Community

This section describes settings that can be configured by selecting Manage > VPN Communities > Remote Access and clicking Edit, or alternatively clicking the VPN Manager tab of the Rule Base pane, right clicking Remote Access and clicking Edit.

Follow the instructions in Introduction to Remote Access VPN, in Chapter 14 of the Virtual Private Networks Administration Guide Version R70 to configure a Remote Access Community.

1. In the Remote Access Community Properties window, name the community.
2. In the **Participating Gateways** window, click **Add** to add the already defined Gateways participating in the Remote Access Community.

New Gateways can be created or existing Gateways added to the list. A member of the community is listed both here and in the **VPN** page of the relevant Gateway object.
3. In the **Participating User Groups** window, click **Add** to add the group that contains the remote access users.

New user groups can be created or existing user groups added to the list.
Configuring Remote Access in Global Properties

1. In the Authentication page:

   - If certificate-based authentication is used for remote access user authentication, you may either disable the **Authenticate internal users with this suffix only** setting, or provide a suffix that matches the remote access user certificate distinguished names (DNs).
2. In the **Remote Access** page:

- Verify that the **Update topology every**… checkbox is not selected.
3. In the **Remote Access– VPN – Authentication and Encryption** page:

<table>
<thead>
<tr>
<th>Global Properties</th>
<th>VPN - Authentication and Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Encryption Method</td>
</tr>
<tr>
<td></td>
<td>□ IKEv2 only (Check Point VPN Clients will not be able to connect)</td>
</tr>
<tr>
<td></td>
<td>□ IKEv2, support IKEv1</td>
</tr>
<tr>
<td></td>
<td>□ IKEv1 only</td>
</tr>
<tr>
<td></td>
<td>Encryption Suite</td>
</tr>
<tr>
<td></td>
<td>□ VPN A (DES, SHA-1, Diffie-Hellman Group 2)</td>
</tr>
<tr>
<td></td>
<td>□ VPN B (AES, AES-XCBC, Diffie-Hellman Group 14)</td>
</tr>
<tr>
<td></td>
<td>□ Custom Advanced</td>
</tr>
<tr>
<td></td>
<td>Support authentication methods</td>
</tr>
<tr>
<td></td>
<td>□ Pre-Shared Secret (For SecureRemote/SecureClient users)</td>
</tr>
<tr>
<td></td>
<td>□ Public Key Signatures</td>
</tr>
<tr>
<td></td>
<td>□ Support Legacy Authentication for SC (Hybrid mode), L2TP [PAP], and Notify clients (CPACK)</td>
</tr>
<tr>
<td></td>
<td>□ Support Legacy EAP</td>
</tr>
<tr>
<td></td>
<td>□ Support L2TP with Pre-Shared Key</td>
</tr>
<tr>
<td></td>
<td>□ IKE over TCP</td>
</tr>
<tr>
<td></td>
<td>□ Gateways support IKE over TCP</td>
</tr>
</tbody>
</table>

- Public Key Signatures are supported by default. Select **Pre-Shared Secret** checkbox, if pre-shared secrets are used for Remote Access authentication.
- Verify that the **Support Legacy EAP** and **Support L2TP with Pre-Shared Key** checkboxes are not selected.

**Note:** Pre-shared secret keys if used should be generated using a cryptographically-strong (FIPS-approved) Random Number Generator (RNG). For example: 40 hexadecimal digits contain the equivalent number of bits to that provided by the SHA-1 hash algorithm.
4. If configuring a **Custom** Encryption Suite (using the **Advanced**... button), verify that **DES** is not selected as a supported encryption algorithm, and that **MD5** is not selected as a supported data integrity algorithm, as these algorithms are not FIPS-Approved.
5. In the Secure Configuration Verification (SCV) page:

- Do not set **Apply Secure Configuration Verification on Simplified mode Security Policies**.
6. In the SSL Network Extender page:

- In the **User authentication method** field, you may select any of the authentication options, with the following qualifications:
  - In the TOE evaluated configuration, “Certificate with enrollment” is equivalent to “Certificate”, as the enrollment protocol will not be supported by the evaluated configuration rule base.
  - If “Legacy” or “Mixed” options are selected for password-based authentication, the administrator should configure single-use password authentication using a RADIUS or SecurID server.
- In the **Supported Encryption methods** field, select **3DES only**.
7. In the **SecureClient Mobile** page:

- In the **Supported Encryption methods** field, select **3DES only**.
20. In the SmartDirectory [LDAP] page:

- Verify that **Use SmartDirectory (LDAP) for Security Gateways**... is not selected.
- Verify that **Use SmartDirectory (LDAP) for SSLVPN**... is not selected.
Defining Remote Access Rules

The existence of a remote access community does not mean that members of that community have free automatic access to the network. Appropriate rules need to be created in the Security Policy Rule Base blocking, or allowing specific services. There must be a rule in the Security Policy Rule Base that grants remote users access to the LAN. Consider which services are allowed. Restrict those services that need to be restricted with an explicit rule in the Security Policy Rule Base. For example, to allow remote access users to access the organization’s SMTP server, called SMTP_SRV, the administrator can create the following rule:

<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>SMTP_SRV</td>
<td>Remote_Access_Community</td>
<td>TCP smtp</td>
<td>Accept</td>
<td>Log</td>
</tr>
</tbody>
</table>
Content Inspection Settings

Content Inspection functionality is outside the evaluated configuration. In the SmartDashboard toolbar, click the Anti-Virus & URL Filtering tab.

1. In the Database Updates window make sure that Automatic Update is not configured.

2. In the SmartDashboard toolbar, click the Anti-Spam & mail tab.

In the Database Updates window make sure that Automatic Update is not configured.
Security Policy Installation

In This Chapter

SIC Trust Establishment  page 134
Security Policy Installation  page 139

SIC Trust Establishment

In order for management communication to be established between the Security Management server and a Security Gateway, Secure Internal Communications (SIC) trust must be established between these components. SIC trust is established by securely downloading a SIC certificate created by the Internal Certificate Authority (ICA) residing on the Security Management server to the Security Gateway.

The ICA certificate download is protected by entering a shared one-time Activation Key on both components. The Activation Key is entered on both components, on the Communication... screen of the Security Gateway object in SmartDashboard (for the Security Management server), and on the cpconfig prompt when installing the Security Gateway (see CC Evaluated Configuration Installation Guide section Installing the Security Gateway). This section describes the process of obtaining a secure Activation Key and of entering it in SmartDashboard.
Obtaining the Activation Key

1. Edit the Gateway network object. Select the object and right click, then select **Edit**.
2. On the Gateway object’s IPSecVPN tab, select the defaultCert in the Certificates List, and click on the View button:

![Check Point Gateway - Gateway](image)

**Note:** If defaultCert does not appear in the Certificates List, this indicates that the administrator failed to set VPN in the Check Point Products list of the Check Point Gateway – General Properties window, or that the Gateway object has not been created. Complete the definition of the object and retry this step.
3. Scroll down in the **Certificate View** Window all the way to the bottom of the window. The certificate Fingerprint is displayed in 2 formats: hexadecimal octet format, and mnemonic format:

![Certificate View](image)

4. Copy the fingerprint (either one) into the SmartConsole host’s paste buffer: select the certificate fingerprint string, right click on the selection and select **Copy**. Click **OK**.

**Note**: A new ICA certificate is automatically created for the Security Gateway whenever SIC trust must be re-established. The certificate fingerprint is a strong random sequence, generated by a FIPS-approved random number generator, and providing 20 octets-worth of random information. Because this sequence is known only to the Security Management server before SIC trust has been successfully established, it is suitable for serving as the basis for the secure trust establishment with the Security Gateway.

**Trust Establishment**

1. Enter the Activation Key on the cpconfig prompt on the Security Gateway. Complete the installation of the Security Gateway, as described in the *CC Evaluated Configuration Installation Guide*. 
Note: You may find it helpful to paste the Activation Key into a text file that can be printed or displayed while completing the cpconfig prompt.

2. Edit the Security Gateway gateway object. Select the Communication… button:

![Image of Communication dialog box](image1)

3. Paste the Certificate string you have previously stored in the paste buffer into the Activation key box, paste it again to the Confirm Activation key box, and select Initialize:

![Image of Communication dialog box with Activation Key](image2)
4. You will see the message **Trust established**. Select **Close** to close the **Communication…** window.

![Communication Window](image)

**Security Policy Installation**

Once the evaluated configuration Security Policy package is ready for installation, the Security Gateway has completed installation, and SIC trust has been established, follow the instructions given in Working with Policies, in Chapter 1 of the *Check Point Security Management Server R71 Administration Guide* to install the Security Policy on the Security Gateway.

**Note:** Some configurations require the Security Policy to be installed on multiple Security Gateway for it to be effective. For example, this is certainly the case where two Security Gateway participate in the same VPN community.
Monitoring
CHAPTER 11

Monitoring System Status

SmartView Monitor

Overview

SmartView Monitor is a high-performance network and security-analysis system that helps Security Administrators administer their networks. SmartView Monitor allows administrators to easily configure and monitor different aspects of network activities.

Pre-defined views include the most frequently used traffic, counter, tunnel, gateway, and remote user information. For example, Check Point System Counters collect information on the status and activities of Check Point products (for example, VPN-1 Power, etc.). Using custom or pre-defined views, administrators can drill down on the status of a specific gateway and/or a segment of traffic to identify top bandwidth hosts that may be affecting network performance. If suspicious activity is detected, administrators can immediately apply a security rule to the appropriate Check Point gateway to block that activity. These security rules can be created dynamically via the graphical interface and be set to expire within a certain time period.

For detailed information on configuration and uses of SmartView Monitor, refer to the Check Point SmartView Monitor R71 Administration Guide.
You can monitor:

- Alerts
- Gateways
- Traffic
- Tunnels
- Remote Users
Alerts

Alerts are generated when the Security Policy specifies Alert or SnmpAlert in the Track attribute for a given security-relevant event. In addition, the administrator can set up thresholds in SmartView Monitor for monitored resources, so that alerts are generated when resources exceed set thresholds.

**Note:** Perform Start System Alert Daemon from the Tools menu to activate threshold monitoring.

Pop-up Alerts are displayed in the Alerts window in SmartView Monitor. By default, pop-up Alerts cause SmartView Monitor to play a special sound, and to pop up the Alerts window. This behavior can be inhibited by the administrator. The administrator can selectively delete alerts from the pop-up Alerts window.

![Alerts Window](image)

**Note:** Pop-up Alerts will not be displayed if there is no SmartView Monitor application open at the time the Alert is generated. However, they will still appear in the log and can be reviewed after the fact using SmartView Tracker.

SNMP Alerts are sent to a defined SNMP catcher host.
Status Displays

When discussing the status of the monitored appliances and hosts, there are general statuses which occur for both the machine on which the Check Point software is installed, and the product which represents the applications installed on the machine.

- **Waiting** – from the time that the view starts to run until the time that the first status message is received.
- **OK** – target is responding to status update requests from the Security Management server.
- **Attention** – ClusterXL related status
- **No License** – license-related problem reported.
- **Above Threshold** – target resource levels have exceeded a defined threshold.
- **Warning/Problem/Critical Problem** – target is responding to status update requests, but a product-specific problem (e.g. "policy not installed") is being reported.
- **Untrusted** – Secure Internal Communication failed. The machine is connected, but the Security Management server is not the master of the module installed on the machine.
- **Unknown** – the machine cannot be reached or there is no Check Point agent installed on it.
Gateway Information

In SmartView Monitor - Gateways, information is displayed per Check Point host. To display information about the host, click the specific host in the Gateways Results view. Elaborate details about the host will be displayed in the adjacent Gateway Details window. This information includes general information such as the name, IP Address, version, OS and the status of the specified host, or host specific information, such as:

- **Unified Package** - the version number.
- **OS Information** - the name, the version name/number, the build number, the service pack and any additional information about the Operating System in use.
- **CPU** - the percentage of CPU consumption in general and specifically by the user, by the system, and the amount of time that the CPU has been idle.
- **Memory** - the total amount of virtual memory, what percentage of this total is being used. The total amount of real memory, what percentage of this total is being used, the amount of real memory available for use.
- **Disk** - the percentage/total of free space on the disk, the total amount of free space, as well as the actual amount of free space available for use.
CHAPTER 12

Monitoring Traffic

SmartView Tracker

Overview

The SmartView Tracker can be used to track all daily network traffic and activity logged by Check Point products. It can also be used to give an indication of certain problems.

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. The modules on which the Security Policy (derived from the Rule Base), is installed collect data as specified in the Policy, and forward the logs to the Security Management server. 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.

For detailed information on configuration and uses of SmartView Tracker, refer to the Check Point Security Management Server R71 Administration Guide.
Log Record Attributes

Log records have a variable format consisting of a set of typed named attributes, as appropriate to the reported event. All log records include a log Number in the viewed log file, and Date and Time attributes that are stamped by the host that generated the record (Origin).

Note: If an NTP server is not used to synchronize clocks between different hosts, clock drift might cause records generated by one host to receive time stamps that are later than those generated by another host, even if the latter records were generated later than the former. Use the Origin attribute to distinguish between these records. Also note that the records are displayed in the order in which they were received by the Security Management server.
Action Column

The Action column describes the action taken by the Check Point Software Blades R7x appliance that generated the log record, in response to the connection request. For each Log record, SmartView Tracker displays an Action value and a representative icon. Relevant values are:

- **Accept** – the connection was allowed by the Security Policy Rule Base;
- **Reject/Drop** – connection was rejected or dropped by the Security Policy. Note that this connection may or may not have matched a VPN community definition. It is possible to determine this from other fields, e.g. by reference to the matched rule, or by whether the User column identifies a Remote Access user DN.
- **Encrypt/Decrypt** – the connection was allowed by the Security Policy, and has been protected by an IPSec VPN tunnel. The IPSec peer through which the connection was encrypted generates an Encrypt log, and the peer that decrypts the connection generates a corresponding Decrypt log;
- **Key Install** – an IKE event, including SA creation, IKE session establishment failure, and other IKE-related events (e.g. CRL pre-fetch failure).
Rule Base Rule Columns

SmartView Tracker records the Security Rule Base rule to which a connection was matched. The matching rule is recorded in four columns in SmartView Tracker:

- **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.
- **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.
Appendices
APPENDIX A

Management Functions

In This Chapter

Security Policy installation and policy revision control  page 155
Management of multiple authentication mechanisms  page 155
Management of audit generation settings  page 158
Control of communication with external IT entities  page 158
Modification of IPS System behavior  page 160
Enabling or disabling Security Policy implied rules  page 161
Enabling SIC connectivity  page 161
Management of Rule Base and VPN Communities  page 162
User management  page 163
Object database management  page 163
Audit trail management  page 163
Exporting log records to a file  page 164
Performing audit queries  page 164
Defining monitoring thresholds for resource values  page 165
Monitoring resource levels and connectivity status  page 165
Viewing alerts  page 165
Fault Tolerance  page 166
This appendix provides additional references to guidance provided in this document and other Check Point documentation, for each of the security-relevant management functions identified in CHAPTER 3.

These references are intended to aid the administrator in identifying applicable guidance for performing security-relevant administration tasks.

**Security Policy installation and policy revision control**

Security policies are created by the system administrator on the Security Management server and distributed (installed) to Security Gateway that enforce the policy.

Different versions of these policies can be saved. Each version includes backups of the various databases (objects, users, Certificate Authority data, etc.). The 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, view a version, revert to a previous version and delete a version.

Security Policy installation is described in:

*Security Management Server*
Chapter 1, *Security Management Overview / Working with Policies*

Policy revision control is described in:

*Security Management Server*
Chapter 7, *Policy Backup and Version Control*

**Management of multiple authentication mechanisms**

The Check Point Software Blades R7x product supports a wide range of authentication mechanisms. The following mechanisms are considered to be part of the evaluated configuration:

- Administrators authenticating via SmartConsole using certificates issued by the Internal Certificate Authority (ICA);
- Remote access (SecuRemote/SecureClient) users authenticating using IKE certificates issued by trusted external CAs, or using pre-shared secret authentication;
- FTP and Telnet users authenticating using a single-use password mechanism, validated using a RADIUS or SecurID authentication server;
- Peer VPN gateways authenticating over IKE using IKE certificates issued by trusted external CAs, or using pre-shared secret authentication;
- RADIUS server authenticating using MD5 Shared Secret
- NTP server authenticating using MD5 Shared Secret (established during the installation phase)

Management of administrator authentication credentials is discussed in:

*CC Evaluated Configuration Administration Guide*

*CHAPTER 3, Administration Interfaces / Administrator Accounts*

*Security Management Server*

Chapter 1, *Security Management Overview / Managing Users in SmartDashboard / Configuring User Objects / Configuring Administrators*

Chapter 4, *The Internal Certificate Authority (ICA) and the ICA Management Tool / The ICA Solution / User Certificate Management*

Management of Remote Access user authentication credentials is described in:

*CC Evaluated Configuration Administration Guide*

*CHAPTER 8, Remote Access VPN / User Configuration*

*Virtual Private Networks*

Chapter 14, *Introduction to Remote Access VPN / VPN for Remote Access Configuration / Configure Certificates Using Third Party PKI Using a Pre-Shared Secret*
Management of FTP and Telnet users' single-use password authentication credentials is described in:

*CC Evaluated Configuration Administration Guide*

*CHAPTER 5, Authenticated Services / User Configuration*

**Firewall**

Chapter 2, *Authentication /*

- Configuring User Authentication
- Configuring a Security Gateway to use RADIUS
- Granting User Access Using RADIUS Server Groups
- Configuring a Security Gateway to use SecureID

Management of VPN peer authentication credentials is described in:

*Virtual Private Networks*

Chapter 4, *Introduction to Site to Site VPN /*

- Configuring a VPN with External Gateways Using PKI
- Configuring a VPN with External Gateways Using a Pre-Shared Secret

Management of RADIUS server MD5 Shared Secret is described in:

*CC Evaluated Configuration Administration Guide*

*CHAPTER 5, Authenticated Services / Authentication Server Configuration*

**Firewall**

Chapter 2, *Authentication /*

- Configuring a Security Gateway to use RADIUS

Management of NTP server MD5 Shared Secret is described in:

*CC Evaluated Configuration Installation Guide*

*CHAPTER 5, R71 Fresh Installation /*
Installing Security Management server
Installing the Security Gateway

Management of audit generation settings

Logs are generated on both the Security Management server and Security Gateway. Logging is configured using SmartDashboard.

Logging settings for SmartDashboard are described in:
*CC Evaluated Configuration Administration Guide*
CHAPTER 4, *Creating the Security Policy / Configuring the Primary Management Object*
*Creating the Security Cluster or Gateway Objects*

*Security Management Server*
Chapter 5, *SmartView Tracker / Tracking Configuration / Maintenance*
*Working with Log Servers*
*Local Logging*

Control of communication with external IT entities

External IT entities that communicate with the evaluated configuration must be defined as objects using SmartDashboard, and appropriate information flow rules configured to allow this communication.

An overview of the types of authorized external IT entities that may communicate with the evaluated configuration is provided in:
*CC Evaluated Configuration Installation Guide*
CHAPTER 1, *Evaluated Configuration / Physical Components of the Evaluated Configuration*

Security Policy Rules that allow such communication are defined in:
*CC Evaluated Configuration Administration Guide*
CHAPTER 4, *Creating the Security Policy / Management Rules /
NTP Rule
Authentication Server Rules
VPN Rules
IPS Updates Rules
CVP and UFP Rules

Parameters for NTP server communication are identified in:
*CC Evaluated Configuration Installation Guide*
CHAPTER 5, R71 *Fresh Installation /
Installing Security Management server
Installing the Security Gateway*

Definition of Authentication Server objects is explained in:
*CC Evaluated Configuration Administration Guide*
CHAPTER 5, *Authenticated Services / Authentication Server
Configuration*

*Firewall*
Chapter 2, *Authentication / Configuring Authentication /
Configuring a Security Gateway to use RADIUS
Configuring a Security Gateway to use SecureID*

A general overview of VPN communities is provided in:
*Virtual Private Networks*
Chapter 1, *Overview
Chapter 4, Introduction to Site to Site VPN / VPN Communities*

Definition of object and VPN community definitions needed for establishing communication with VPN peers is described in:
*CC Evaluated Configuration Administration Guide*
CHAPTER 7, *Site to Site VPNs*
Communication with CVP and UFP servers is controlled via Resource objects, described in:

*CC Evaluated Configuration Administration Guide*

CHAPTER 5, *Authenticated Services / Resource Definition*

**Firewall**

Chapter 14, *Content Security*

### Modification of IPS System behavior

SmartDashboard provides the authorized administrator with the ability to define and modify services that match traffic patterns that may be indicative of intrusion or other malicious activity.

The IPS Update capability allows the administrator to import IDS signature updates from a file. The updates are provided by Check Point in response to newly discovered published attacks and/or vulnerabilities.

An overview of the IPS capability is provided in:

*IPS Administration Guide*

Evaluated configuration settings for IPS are described in:

*CC Evaluated Configuration Administration Guide*

CHAPTER 6, *IPS Settings*
Enabling or disabling Security Policy implied rules

An overview of the Implied Rules capability is provided in:

*Firewall*

Chapter 1, *Access Control / Solution for Secure Access Control / Implied Rules*

Constraints on the definition of Implied Rules in the evaluated configuration are indicated in:

*CC Evaluated Configuration Administration Guide*

CHAPTER 4, *Creating the Security Policy / Defining Global Properties*

Enabling SIC connectivity

Secure connectivity between the Security Management server and Security Gateway is based on the Secure Internal Communications (SIC) facility. SIC certificates are issued by the Internal CA (ICA) on the Security Management server, and distributed to Security Gateway.

Initial trust establishment between the Security Gateway and the Security Management server consists of entering an Activation key during Security Gateway installation, and entering the same Activation Key in SmartDashboard.

The trust establishment process is described in:

*Security Management Server*

Chapter 1, *Security Management Overview / Securing Channels of Communication (SIC)*

*CC Evaluated Configuration Installation Guide*

CHAPTER 5, R71 *Fresh Installation / Installing the Security Gateway*
Management of Rule Base and VPN Communities

The Security Policy is implemented by defining an ordered set of rules in the Security Rule Base. The Rule Base specifies what communication will be allowed to pass and what communication will be blocked. Each rule also specifies whether matched traffic will be logged, and whether an Alert will be generated.

VPN Community definitions control the establishment of VPN tunnels with peer VPN gateways and remote access clients.

Management of the Security Policy is described in:

*Firewall*
  - Chapter 1, *Access Control*

*CC Evaluated Configuration Administration Guide*
  - CHAPTER 4, *Creating the Security Policy*

VPN Communities are described in:

*Virtual Private Networks*
  - Chapter 4, *Introduction to Site-to-Site VPN*
  - Chapter 14, *Introduction to Remote Access VPN Overview*

*CC Evaluated Configuration Administration Guide*
  - CHAPTER 7, *Site to Site VPNs*
  - CHAPTER 8, *Remote Access VPN*
User management

User management is described in:

- **Security Management Server**
  - Chapter 1, *Security Management Overview / Managing Users in SmartDashboard*

- **Firewall**
  - Chapter 2, *Authentication / Creating Users and Groups*

- **CC Evaluated Configuration Administration Guide**
  - CHAPTER 3, *Administration Interfaces / Administrator Access Control Permissions Profiles Administrator Accounts*
  - CHAPTER 5, *Authenticated Services, User Configuration*

Object database management

Managing objects in the Objects Database is described in:

- **Security Management Server**
  - Chapter 1, *Security Management Overview / Managing Objects*

- **CC Evaluated Configuration Administration Guide**
  - CHAPTER 4, *Creating the Security Policy / Defining Management Objects*

Audit trail management

SmartView Tracker allows the authorized administrator to perform log management functions that include:

- Performing log switch and log purge operations on active log files
- Manually fetching log files from Security Gateway

Log file management is described in:
Old log files on the Security Management server can be deleted by the authorized administrator using appropriate log setting operations - see: 
*CC Evaluated Configuration Administration Guide*
CHAPTER 4, *Creating the Security Policy / Defining Management Objects*

**Exporting log records to a file**

Exporting log records to a file:
*Security Management Server*
Chapter 5, *SmartView Tracker / The Check Point Solution for Tracking / Log Export Capabilities*

**Performing audit queries**

SmartView Tracker provides extensive audit query facilities, including filter and search capabilities. See:
*CC Evaluated Configuration Administration Guide*
CHAPTER 12, *Monitoring Traffic*

*Security Management Server*
Chapter 5, *SmartView Tracker / The Check Point Solution for Tracking /*

*SmartView Tracker*
Filtering
Queries
Matching Rule
Chapter 5, SmartView Tracker / Tracking Configuration /
Basic Tracking Configuration
SmartView Tracker View Options
Configuring a Filter
Configuring Queries
Hiding and Showing the Query Tree Pane
Working with the Query Properties Pane
Modifying a Columns Properties
Viewing a Record's Details
Viewing a Rule
Find by Interface

Defining monitoring thresholds for resource values
Definition of thresholds in SmartView Monitor is described in:
SmartView Monitor
Chapter 3, Monitoring Gateway Status / Configuring Gateway Views /
Defining a Threshold
Define Global Threshold Settings

Monitoring resource levels and connectivity status
SmartView Monitor allows the administrator to monitor resource levels on
the Security Management server and Security Gateway. See:
CC Evaluated Configuration Administration Guide
CHAPTER 11, Monitoring System Status

SmartView Monitor
Chapter 3, Monitoring Gateway Status /
Displaying Gateway Information
Views about a Specific Gateway

Viewing alerts
Popup Alerts are displayed in real-time in the Alerts window of the
SmartView Monitor Management GUI.
The Alerts window is described in:

- *SmartView Monitor*
  Chapter 5, *Monitoring Gateways Status / Alert Dialog*

- *CC Evaluated Configuration Administration Guide*
  CHAPTER 11, *Monitoring System Status / SmartView Monitor / Alerts*

**Fault Tolerance**

Configuration and monitoring of Management High Availability is described in:

- *Security Management Server*
  Chapter 1, *Management High Availability*

Configuration and monitoring of gateway clusters is described in:

- *ClusterXL R70.1*
notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.


Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

The curl license

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2004, Daniel Stenberg, <daniel@haxx.se> All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

The PHP License, version 3.0

Copyright (c) 1999 - 2004 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/ or other materials provided with the distribution.

3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "

This product includes PHP, freely available from <http://www.php.net/>."

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
THE MATERIAL IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND EITHER EXPRESS OR IMPLIED. TO THE
FULLEST EXTENT POSSIBLE PURSUANT TO THE APPLICABLE LAW, NEXTHOP DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED,
INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON INFRINGEMENT
OR OTHER VIOLATION OF RIGHTS. NEITHER NEXTHOP NOR ANY OTHER PROVIDER OR DEVELOPER OF MATERIAL CONTAINED IN THIS
DOCUMENT WARRANTS OR MAKES ANY REPRESENTATIONS REGARDING THE USE, VALIDITY, ACCURACY, OR RELIABILITY OF, OR THE
RESULTS OF THE USE OF, OR OTHERWISE RESPECTING, THE MATERIAL IN THIS DOCUMENT.

Limitation of Liability

UNDER NO CIRCUMSTANCES SHALL NEXTHOP BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES,
INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA OR PROFIT, ARISING OUT OF THE USE, OR THE INABILITY TO USE, THE MATERIAL IN THIS
DOCUMENT, EVEN IF NEXTHOP OR A NEXTHOP AUTHORIZED REPRESENTATIVE HAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IF
YOUR USE OF MATERIAL FROM THIS DOCUMENT RESULTS IN THE NEED FOR SERVICING, REPAIR OR CORRECTION OF EQUIPMENT OR DATA,
YOU ASSUME ANY COSTS THEREOF. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL
DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT FULLY APPLY TO YOU.

Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.
BIND: ISC Bind (Copyright (c) 2004 by Internet Systems Consortium, Inc. ("ISC"))
Copyright 1997-2001, Theo de Raadt: the OpenBSD 2.9 Release

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language. Release 5
of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed
under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>
Copyright (c) 1997-2004 University of Cambridge All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or
  other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.