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..................... 15
SmartCenter Server............................................................ 16
SmartConsole (Management GUI) ....................................16

CHAPTER 3  Administration Interfaces
Management Functionality ................................................ 17
SmartConsole..................................................................... 19
Administrator Access Control............................................ 20
Permissions Profiles........................................................... 21
Administrator Accounts..................................................... 22

Security Policy

CHAPTER 4  Creating the Security Policy
Security Policy Considerations........................................... 25
Defining Basic Objects...................................................... 26
Defining Global Properties ................................................ 43
Defining Rules................................................................. 50
Creating a Policy Package................................................ 50
Management Rules ........................................................... 51

CHAPTER 5  Authenticated Services
SmartView Tracker .......................................................... 130

SmartDefense ........................................................................ 135

CHAPTER 13 SmartDefense Updates ................................................. 137
Overview .............................................................................. 137
Offline Update ................................................................. 138
Downloading the SmartDefense Update .................................. 139
Loading the SmartDefense Update ....................................... 140
Defining Manual IDS Match Strings ................................... 141

Appendices ............................................................................. 143

APPENDIX A Management Functions ...................................... 145
Security Policy installation and policy revision control... 146
Management of multiple authentication mechanisms ...... 146
Management of audit generation settings ......................... 149
Control of communication with external IT entities ............ 149
Modification of IDS System behavior ............................... 151
Enabling or disabling Security Policy implied rules .......... 152
Enabling SIC connectivity .................................................... 152
Management of Rule Base and VPN Communities .......... 153
User management ............................................................. 154
Object database management ............................................ 154
Audit trail management ....................................................... 154
Exporting log records to a file ............................................. 155
Performing audit queries ..................................................... 155
Defining monitoring thresholds for resource values ........... 156
Monitoring resource levels and connectivity status .......... 156
Viewing alerts ................................................................. 156
The Common Criteria Evaluated Configuration
Overview

In This Chapter

The Certification Challenge
Reference Material
How to use this Administration Guide

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 VPN-1 Power/UTM NGX R65 in accordance with the Common Criteria evaluated configuration, as defined in the Check Point VPN-1 Power/UTM NGX R65 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 VPN-1 Power/UTM NGX R65 Security Target

Installation guidance is provided in:
- Check Point CC Evaluated Configuration Installation Guide

See the following Check Point documentation provided on the product CD-ROMs for more information on Check Point VPN-1 Power/UTM NGX R65 administration:
- SmartCenter
- Firewall and SmartDefense
- Virtual Private Networks
- SmartView Monitor

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 enforcement modules 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 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, IDS/IPS functionality (SmartDefense), 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 10 Security Policy Installation provides instructions for setting up Secure Internal Communications (SIC) trust between the SmartCenter Server and enforcement modules, and for installing the Security Policy on the enforcement module.

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 13 SmartDefense UpdatesCHAPTER 13 provides instructions for loading SmartDefense Update files and for defining manual IDS match strings.
CHAPTER 2

Physical Boundaries

In This Chapter

Components of the Evaluated Configuration page 15
SmartCenter Server page 16
SmartConsole (Management GUI) page 16

Components of the Evaluated Configuration
The evaluated configuration includes the following components:

- **Enforcement Module** - Check Point VPN-1 Power/UTM NGX R65 software installed on an appliance running the Check Point SecurePlatform NGX R65 operating system
- **SmartCenter Server** - management server software installed on a host running the Check Point SecurePlatform NGX R65 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.

An evaluated configuration includes one SmartCenter Server, one or more Enforcement Modules, and one or more SmartConsoles.
**SmartCenter Server**

The Check Point VPN-1 Power/UTM NGX R65 media includes management server software, SmartCenter Server. A SmartCenter Server manages one or more Check Point VPN-1 Power/UTM NGX R65 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 SmartCenter 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 VPN-1 Power/UTM NGX R65 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 SmartCenter 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 SmartCenter Server or enforcement module consoles. SmartConsole certificate-based login should be used exclusively.

It is recommended that administrators should *not* be provided console login and cpconfig administrator passwords.
In This Chapter

Management Functionality
SmartConsole
Administrator Access Control
Permissions Profiles
Administrator Accounts

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 VPN-1 Power/UTM NGX R65 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 VPN-1 Power/UTM NGX R65 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 SmartCenter 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 SmartCenter Server.

The abstract Security Policy is translated by the SmartCenter 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 VPN-1 Power/UTM NGX R65 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
- management of multiple authentication mechanisms
- management of audit generation settings
- control of communication with external IT entities
- modification of IDS System behavior
- enabling or disabling Security Policy implied rules
- enabling SIC connectivity
- Management of Rule Base and VPN Communities
- user management
- 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 SmartCenter Server maintains a user database. The user database is distributed to the evaluated configuration’s Check Point VPN-1 Power/UTM NGX R65 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 SmartCenter 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
Audit Administrator 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 SmartCenter Server or on enforcement modules 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 should not receive any alternative authentication scheme. Verify that the **Authentication Scheme** is **Undefined** in the **Admin Auth** 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

- Security Policy Considerations  page 25
- Defining Basic Objects  page 26
- Defining Global Properties  page 43
- Defining Rules  page 50
- Creating a Policy Package  page 50
- Management Rules  page 51

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 (gateways, networks, routers, domains)

Security Policy creation entails the following steps:

- Defining Basic 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 enforcement module. 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 SmartCenter Server and enforcement modules, 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 SmartCenter Server.

Follow the instructions provided in Configuring Objects, in Chapter 1 of the *Check Point SmartCenter Guide* to define Basic Objects.

In the evaluated configuration, you will be defining various objects, including: a Management Module, at least one Enforcement Module, 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.
Configuring the Management Object

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

2. Configure the General Properties page:
Set only the Log Server check box under Check Point Products. **Note:** In the evaluated configuration, the Management Object should **not** be defined as a Gateway – do **not** set the Firewall and VPN check boxes for the Management Object. Do not configure additional Web, Mail, or DNS servers on the Management Object.

3. Configure the Topology page: select Add… and specify the Name, IP Address, and Net Mask for the SmartCenter Server host network interface.

4. Configure the Logs and Masters page:
Notes: In the evaluated configuration, there is no direct administrator interface for manually deleting or purging log files on the SmartCenter Server. These files accumulate both from audit files generated by the SmartCenter Server, and from log files forwarded by the enforcement modules.

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 SmartCenter 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 SmartCenter 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 enforcement modules when free disk space on the SmartCenter Server is below an administrator-defined value. The log records will still be accumulated on the enforcement modules; 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 _**.
Creating the Security Gateway Object

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

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.

To define the gateway object, perform the following steps:

1. From the Objects Tree in SmartDashboard, right click Network Objects and select New > Check Point > VPN-1 Pro/Express Gateway.
2. Alternatively, you can select Network Objects from the Manage menu. The Network Objects window appears.
3. Click New and select Check Point > VPN-1 Pro/Express Gateway. A window is displayed which allows you to configure this object using a wizard, or manually, via the Classic method.
4. Select the Classic method. The Check Point Gateway General Properties page is displayed.
5. Configure the **General Properties** page:

Set only the **Firewall**, **VPN**, and **SmartView Monitor** (optional) check boxes under Check Point Products.

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

- Configure the relevant interfaces.
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 define 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 enforcement module.
7. In the Logs and Masters page:

- Do not set Required Free Disk Space on the enforcement module; 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 enforcement module. 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 enforcement module disk resources are running out. When such an alarm is generated, verify that scheduled log forwarding is enabled to send log files to the SmartCenter Server (see below). You can also use the SmartView Tracker **Remote Files Management...** command to fetch log files from the enforcement module, freeing up local storage.
8. In the **Additional Logging Configuration** page:

- Set **Forward log files to the SmartCenter Server**. Select the Management host in the drop down menu. Select an appropriate log forwarding schedule (e.g. 'Midnight').
- Set **Perform Log switch before log forwarding**.
9. In the Log Servers page:

- Do not set **Use local definitions for Log Servers**.
- Set **Save logs locally, on this machine**.
- Verify that the **Always send logs to** setting for the Log Server (SmartCenter Server) object includes both Logs and Alerts, as depicted above.
10. In the **Cooperative Enforcement** page:

- Do *not* set **Authorize clients using Integrity 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 Additional Basic Objects**

1. Define all Hosts, Clients, Client Networks, Ranges and other network objects, to be used either as Source or Destination in the Rule Base.

**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 VPN-1 Power/UTM NGX R65 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.
1. In the **FireWall** page:

- Verify that **Accept VPN-1 Power/UTM control connections** is not selected.
- Verify that **Accept outgoing packets originating from Gateway** is not selected.
- Verify that **Accept SmartUpdate connections** is not selected.
- Verify that **Accept VRRP packets...** is not selected.
2. 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;</td>
</tr>
<tr>
<td></td>
<td>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
3. In the **OPSEC** page:

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

- Verify that `http_activate_ss_protections` is selected.

5. Select **FireWall-1 > Security Servers > SMTP Security Server**:

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

Follow the instructions in Configuring Access Control, in Chapter 1 of the *Check Point FireWall and SmartDefense 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 VPN-1 Power/UTM NGX R65 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 Enforcement modules. They can be installed or uninstalled together on selected enforcement modules.

Follow the instructions in Working with Policies, in Chapter 1 of the *Check Point SmartCenter Guide* to create a Policy Package.

**Warning:** Uninstalling the Policy Package from a Check Point VPN-1 Power/UTM NGX R65 appliance removes all Rule Base enforcement functionality; IP forwarding is disabled.
Management Rules

Since Accept VPN-1 Power/UTM control connections has been disabled, you must explicitly allow the following management rules in the Rule Base, to allow VPN-1 enforcement modules and the SmartCenter 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** - A host on which SmartConsole clients are installed. This can be a group of more than one client, defined as GUI clients.
- **Mgmt_server** – The SmartCenter Server network object.
- **FireWalled_modules** – A group of the FireWall-1/VPN gateway objects managed by the Management Module.
- **Revocation_Repository** – Location where CRL is stored.
- **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.

This section lists rules that should be defined to allow management traffic between SmartCenter 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 SmartCenter 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 SmartCenter Server is installed on a protected subnet that is directly connected to a Check Point VPN-1 Power/UTM NGX R65 appliance. The appliance protects the SmartCenter Server from any network access by untrusted users. Do not allow any rules whose destination is the appliance or the SmartCenter 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 SmartCenter Server and Appliances**

The following rules must be defined by the Administrator in order to allow management traffic between the SmartCenter 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>CPD</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CPD_amon</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FW1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FW1_ica_push</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FW1_sam</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FireWalled_modules</td>
<td>Mgmt_server</td>
<td>Any</td>
<td>CPD</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FW1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FW1_log</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Remote Administration Rule

If Remote Administration (see *CC Evaluated Configuration Installation Guide CHAPTER 4 - Deployment*) is to be configured, use the local GUI_client to define a meshed community for management GUIs, e.g. 'CPMI-Community'. (To configure VPN, follow the instructions provided in *CHAPTER 8 - Site to Site VPNs*.) Define the management subnet and any remote GUI subnets to be part of this community. Define in the community properties that 3DES must be used. Specify this community in the VPN column of the following Remote Administration rule:

<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>CPMI_Comm</td>
<td>TCP</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

Management Protection Rule

The following rule protects the SmartCenter 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 SmartCenter 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</td>
<td>snmp-trap</td>
<td>Accept</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 SmartCenter 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, FireWalled_modules</td>
<td>NTP_Servers</td>
<td>Any</td>
<td>UDP ntp-udp</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>IKE_udp</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IKE_NAT_TRAVERSAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IKE_tcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any</td>
<td>ThisModule</td>
<td>Any</td>
<td>IKE_udp</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IKE_NAT_TRAVERSAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IKE_tcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FireWalled_modules</td>
<td>FireWalled_modules</td>
<td>All_GwToGw</td>
<td>tunnel_test</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>Any</td>
<td>FireWalled_modules</td>
<td>RemoteAccess</td>
<td>tunnel_test</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.
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>FireWalled_modules</td>
<td>Revocation_Repository</td>
<td>Any</td>
<td>TCP http</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TCP ldap</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TCP ocsp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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>FireWalled_modules</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>FireWalled_modules</td>
<td>Any</td>
<td>TCP FW1_topo</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 enforcement modules as well. For example, a rule allowing http traffic to 'Any' will allow HTTP connections that terminate on the enforcement module itself.

In order to ensure that no unintended connections are allowed into the enforcement module, it is recommended to define the following rule. This rule will drop all traffic into enforcement modules 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', enforcement modules 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</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 enforcement modules 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>FireWalled_modules</td>
<td>RADIUS-Server</td>
<td>Any</td>
<td>UDP RADIUS</td>
<td>Accept</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
The following rule must be defined if SecurID is used to allow access from the enforcement module 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;gateway&gt;</td>
</tr>
</tbody>
</table>

**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>FireWalled_modules</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>FireWalled_modules</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 enforcement modules 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.

---

2 SecurID servers are installed on protected subnets directly connected to the enforcement modules 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.
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'.

![Diagram of management rules](image)

<table>
<thead>
<tr>
<th>Management Rule</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN-1/Firewall-</td>
<td>Night_server</td>
<td>FireVideo_modules</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>- None</td>
<td>Allow authorized management traffic from SmartCenter Server to enforcement modules.</td>
</tr>
<tr>
<td>Management Rule</td>
<td>FireVideo_modules</td>
<td>Night_server</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>- None</td>
<td>Allow authorized management traffic from enforcement modules to SmartCenter Server.</td>
</tr>
<tr>
<td>Management Rule</td>
<td>GUI_clients</td>
<td>Night_server</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>- None</td>
<td>Allow remote administration sessions.</td>
</tr>
<tr>
<td>Management Rule</td>
<td>Any</td>
<td>Night_server</td>
<td>Any Traffic</td>
<td>Any</td>
<td>drop</td>
<td>Alert</td>
<td>Redirect unauthorized traffic to management components.</td>
</tr>
<tr>
<td>SNMP Alerts</td>
<td>Night_server</td>
<td>Any</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>- None</td>
<td>Allow SNMP alerts generated by SmartCenter Server to exit.</td>
</tr>
<tr>
<td>NTP</td>
<td>FireVideo_modules</td>
<td>Any</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>- None</td>
<td>Allow NTP requests to exit.</td>
</tr>
<tr>
<td>VPN Protocols</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Establishment</td>
<td>Any</td>
<td>ThisModule</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>- None</td>
<td>Allow reverse VPN tunnels to peer VPN gateways.</td>
</tr>
<tr>
<td>VPN Tunnel Test</td>
<td>Any</td>
<td>FireVideo_modules</td>
<td>Any Traffic</td>
<td>All/main/Tunnel</td>
<td>accept</td>
<td>- None</td>
<td>Allow tunnel test protocol to establish IPSec tunnels.</td>
</tr>
<tr>
<td>VPN Tunnel Test</td>
<td>Any</td>
<td>FireVideo_modules</td>
<td>Any Traffic</td>
<td>BGP</td>
<td>accept</td>
<td>- None</td>
<td>Allow tunnel test protocol to remote access VPN tunnels.</td>
</tr>
<tr>
<td>Other Management Rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Separation Rule</td>
<td>Any</td>
<td>ThisModule</td>
<td>Any Traffic</td>
<td>Any</td>
<td>drop</td>
<td>Log</td>
<td>Drop all connection attempts to enforcement modules.</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>ThisModule</td>
<td>Server</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>- None</td>
<td>Allow RADIUS authentication rules.</td>
</tr>
</tbody>
</table>
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 selected.

   ![Authentication page screenshot]

   - In the **Enabled Authentication Schemes** area, verify that the **Check Point Password**, **OS Password** and **TACACS** checkboxes are selected.
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 SmartCenter Guide* and in Chapter 2 of the *Check Point FireWall and SmartDefense Guide* to configure authentication.

**Users**

1. In the **Users and Administrators** tab, right click **Users** and select **New User > Standard User**. 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 > Standard User**. 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.

5. In the **Encryption** tab, if explicitly defined encryption properties are assigned, use only **3DES**, **AES-256**, or **AES-128** as the Encryption Algorithm, and **SHA1** as the Data Integrity algorithm.
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.
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 and SmartDefense Guide.
Security Servers Configuration

Security Servers are proxy processes that must run on the evaluated configuration of Check Point VPN-1 Power/UTM NGX R65. 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 **SmartDefense** tab, select **Mail Security Server**:

2. Set **Configurations apply to all connections**.
FTP Security Server Configuration

1. In the **SmartDefense** tab, select **FTP Security Server**:

2. 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 or UFP, a OPSEC Server object must be defined for the CVP or UFP server.

**Note:** CVP and UFP are the only OPSEC APIs supported in the evaluated configuration.

1. From the Objects Tree in SmartDashboard, click the **Servers and OPSEC Applications** tab.
2. Right click **Servers** and select **New > OPSEC Application**. The **OPSEC Application 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 **OPSEC Application**. The **OPSEC Application Properties** window is displayed.
5. In the **Server Entities** tab, you may select **CVP** and **UFP** entity types, as required. Do *not* select any of the other OPSEC application types in either **Server Entities** or **Client Entities** tabs.
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.
SmartDefense Settings

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

Follow the instructions in Configuring SmartDefense, in Chapter 7 of the Check Point FireWall and SmartDefense Guide to configure SmartDefense.

In the SmartDashboard toolbar, click the SmartDefense tab.
1. In the SmartDefense Settings window, select the SmartDefense category to view information about the category. To view details of a specific attack, click [+] to expand the branch, and select the attack.
2. Check the attacks you wish to defend against, and configure Settings for the categories and the specific attacks.
3. You need to reinstall the Security Policy in order to implement changes to the SmartDefense configuration.

Note: Dshield Storm Center functionality is excluded from the evaluated configuration. The Block malicious IPs setting and the Report to DShield settings must be maintained in Inactive mode (default).
Content Inspection Settings

Content Inspection functionality is outside the evaluated configuration.

In the SmartDashboard toolbar, click the Content Inspection tab.
1 In the Database Updates window, do not select the Enable Automatic Updates checkbox and do not use the other controls in this panel.
CHAPTER 8

Site to Site VPNs

In This Chapter

- Defining a Trusted CA page 80
- Defining an LDAP Account Unit page 81
- VPN Configuration between Managed Gateways page 82
- VPN Configuration with Externally Managed Gateways page 84
- Configuring VPN Communities page 84
- Defining VPN in Global Properties page 91
- Implied Rules and VPN page 94
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.

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. Enter the name and IP address of the LDAP Server.
6. Verify that in the **Account Unit usage** area, the **CRL retrieval** checkbox is selected, and the **User Management** checkbox is not selected.
7. In the **Servers** tab, click **Add**. The **LDAP Server Properties** window is displayed.
8. 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.
9. In the **Encryption** tab, based on your LDAP Server configuration, specify use of SSL, fingerprint and encryption strength.
VPN Configuration between Managed Gateways

From the Objects Tree in SmartDashboard, access the VPN page of the Check Point Gateway that is to participate in 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 VPN-1 Power/UTM NGX R65 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 3 of the *Check Point Virtual Private Networks 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 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. Select only **SHA1** 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.
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 *Check Point Virtual Private Networks 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 `VPN Manager` tab of the Rule Base pane.

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 VPN Properties page:

- 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 has been selected in the Perform data integrity with field.
- 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 has been selected in the Perform data integrity with field.
4. 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.
5. 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.
7. In the SmartDirectory [LDAP] page:

- Verify that **SmartDirectory [LDAP]** is selected if using an Account Unit to access VPN CRLs over the LDAP protocol (see above - *Defining an LDAP Account Unit*).

**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.
Remote Access VPN

In This Chapter

- User Configuration
- Configuring Remote Access in the Gateway Object
- Configuring the Remote Access Community
- Configuring Remote Access in Global Properties
- Defining Remote Access Rules

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 SmartCenter Guide and in Chapter 2 of the Check Point FireWall and SmartDefense Guide to configure authentication.

Users

1. In the Users and Administrators tab, right click Users and select New User > Standard User. 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 > Standard User. The User Properties window is displayed.
4. To enable the user to participate in Remote Access VPN, verify that **IKE** is selected in the **User Properties Encryption** tab.

![User Properties Encryption Tab](image)

5. Follow the instructions in Configuring Certificates for Users and Gateway (Using Third Party PKI), in Chapter 14 of the *Check Point Virtual Private Networks Guide* to obtain certificates for users from 3rd party CAs. Also refer to Defining a Trusted CA and Defining an LDAP Account Unit in CHAPTER 8.

**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:
• Verify that the **Support L2TP** checkbox is not selected.
• Note that **Support Visitor Mode** must be selected if SSL Network Extender functionality is required.

2. In the **Office Mode** page:

![Office Mode configuration settings](image)

• 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 SSL Network Extender 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.
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 Check Point Virtual Private Network Guide 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.

![Participating Gateways window](image)

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 – Basic** page:

- 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 Authentication for SC...** checkbox is 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. In the **Remote Access – VPN – IKE (Phase 1)** page:

- In the **Support encryption algorithms** and **Use encryption algorithm** areas, select one or more of **3DES**, **AES-128**, and **AES-256** encryption algorithms.
- In the **Support Data Integrity** and **Use Data Integrity** areas, select only **SHA1**.
5. In the **Remote Access – VPN – IPSEC (Phase 2)** page:

- In the **Encryption Algorithm** field, select one of the following encryption algorithms: **3DES**, **AES-128**, or **AES-256**.
- In the **Data Integrity** field, select **SHA1**.
6. In the Secure Configuration Verification (SCV) page:

- Do not set Apply Secure Configuration Verification on Simplified mode Security Policies.
7. 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**.
8. In the **SecureClient Mobile** page:

- In the **Supported Encryption methods** field, select **3DES only**.
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>
In This Chapter

*SIC Trust Establishment* page 115
*Security Policy Installation* page 121

**SIC Trust Establishment**

In order for management communication to be established between the SmartCenter Server and an enforcement module, 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 SmartCenter Server to the enforcement module.

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 enforcement module object in SmartDashboard (for the SmartCenter Server), and on the cpconfig prompt when installing the enforcement module (see *CC Evaluated Configuration Installation Guide* section *Installing the Enforcement Module*). This section describes the process of obtaining a secure Activation Key and of entering it in SmartDashboard.
Obtaining the Activation Key

1. Click **OK** when you are done defining the security gateway object. The following message box appears to inform the administrator that an ICA certificate will be created for the gateway. Click **OK** to continue:

![Certificate creation confirmation](image1)

Click **OK** again once the certificate creation operation completes:

![Certificate operation succeeded](image2)

2. Edit the Gateway network object. Select the object and right click, then select **Edit**.

![Gateway network editing](image3)
3. On the Gateway object’s VPN tab, select the defaultCert in the Certificates List, and click on the View button:

**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.
4. Scroll down in the **Certificate View** Window all the way to the bottom of the window. The SHA-1 Fingerprint is displayed in 2 formats: hexadecimal octet format, and mnemonic format:

5. 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 enforcement module 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 SmartCenter Server before SIC trust has been successfully established, it is suitable for serving as the basis for the secure trust establishment with the enforcement module.
Trust Establishment

1. Enter the Activation Key on the cpconfig prompt on the enforcement module. Complete the installation of the enforcement module, 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 Enforcement module gateway object. Select the **Communication** button:
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:
4. You will see the message **Trust established**. Select **Close** to close the **Communication…** window.

---

**Security Policy Installation**

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

**Note:** Some configurations require the Security Policy to be installed on multiple enforcement modules for it to be effective. For example, this is certainly the case where two enforcement modules 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 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.

**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 SmartCenter Server.
- **Attention** – ClusterXL related status. Not applicable in the TOE evaluated configuration.
- **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 SmartCenter 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.
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 SmartCenter Server. The SmartCenter 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 SmartCenter 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 SmartCenter Server.
**Action Column**

The Action column describes the action taken by the Check Point VPN-1 Power/UTM NGX R65 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.
SmartDefense
CHAPTER 13

SmartDefense Updates

Overview

Check Point VPN-1 Power/UTM NGX R65 provides integrated IDS/IPS protection that is controlled from the SmartDefense and Web Intelligence tabs of the SmartDashboard application.

Customers with a valid subscription license also receive special SmartDefense Advisories that provide updated protections against newly identified vulnerabilities, as well as information, tools and best practice methods to mitigate different attacks.
Offline Update

SmartDefense Updates are normally downloaded from the Web directly to the SmartConsole host, as described in the *Firewall and SmartDefense* guide. However, this is not allowed in the evaluated configuration - the SmartConsole host is installed on a LAN that is protected by a firewall that is configured not to let this update request go through.

To provide SmartDefense Updates for customers that have no Internet connectivity from their SmartConsole host, Check Point allows customers that have an appropriate SmartDefense EULA (End User License Agreement) to get the updates as offline file.

Do *not* create or modify SmartDefense Update files or load SmartDefense Update files that were not received from Check Point as described in the sections below.
**Downloading the SmartDefense Update**


Click on the sd_updates.upf link and save the file to removable media. Verify the MD5 hash of the downloaded file against the hash displayed on the Check Point Web site, to validate file integrity.
Loading the SmartDefense Update

1. In SmartDashboard on the SmartDefense tab, select **Download Updates**

2. Select **Offline Update**… and open the file downloaded from the Check Point Web site.
3. The new SmartDefense Update version will be displayed. Select **Continue**:
The SmartDefense update will be loaded. New defenses will appear in boldface on the SmartDefense tab in SmartDashboard. Install policy to distribute the update to enforcement modules.

**Defining Manual IDS Match Strings**

In some cases, Check Point SmartDefense advisories contain instructions on setting up Security Policy rules to block attack signatures that are not automatically detected by the latest SmartDefense Update available on the Check Point Web site.

A powerful tool available for this purpose in SmartDashboard is the definition of services of type 'Other':

![Other Service Properties dialog box](image-url)
The administrator can enter an attack signature string using the Advanced… feature. Attack signature strings are coded in a Check Point proprietary INSPECT language. They are entered in the Match field of the Advanced Other Service Properties window:

In the evaluated configuration, use this functionality only to enter match strings that have been received from Check Point. Take care to enter match strings exactly, character by character. It is recommended to cut & paste match strings from the Check Point advisory into the Match field, rather than typing them in manually.
Appendices
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 SmartCenter Server and distributed (installed) to enforcement modules 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:

*SmartCenter*

Chapter 1, *SmartCenter Overview / Working with Policies*

Policy revision control is described in:

*SmartCenter*

Chapter 2, *Policy Management*

Chapter 6, *SmartCenter Management*

**Management of multiple authentication mechanisms**

The Check Point VPN-1 Power/UTM NGX R65 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

*SmartCenter*
Chapter 1, *SmartCenter 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 9, Remote Access VPN / User Configuration

*Virtual Private Networks*
Chapter 14, *Introduction to Remote Access VPN / VPN for Remote Access Configuration / Configuring Certificates for Users and Gateway (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 and SmartDefense*

Chapter 2, Authentication / Configuring Authentication /
Configuring User Authentication
Configuring a VPN-1 Gateway to use RADIUS
Granting User Access Based on RADIUS Server Groups
Configuring a VPN-1 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 and SmartDefense*

Chapter 2, Authentication / Configuring Authentication /
Configuring a VPN-1 Gateway to use RADIUS

Management of NTP server MD5 Shared Secret is described in:

*CC Evaluated Configuration Installation Guide*

CHAPTER 6, NGX R65 Fresh Installation /
Installing SmartCenter Server
Installing the Enforcement Module
Management of audit generation settings

Logs are generated on both the SmartCenter Server and enforcement modules. 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 Management Object
Creating the Security Gateway Object

SmartCenter
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 2, 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
CVP and UFP Rules

Parameters for NTP server communication are identified in:
CC Evaluated Configuration Installation Guide
CHAPTER 6, NGX R65 Fresh Installation /
Installing SmartCenter Server
Installing the Enforcement Module

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

Firewall and SmartDefense
Chapter 2, Authentication / Configuring Authentication /
Configuring a VPN-1 Gateway to use RADIUS
Configuring a VPN-1 Gateway to use SecureID

A general overview of VPN communities is provided in:
Virtual Private Networks
Chapter 4, Introduction to Site to Site VPN / The Check Point
Solution for VPN

Definition of object and VPN community definitions needed for establishing communication with VPN peers is described in:
CC Evaluated Configuration Administration Guide
CHAPTER 8, Site to Site VPNs

Virtual Private Networks
Chapter 2, IPSEC and IKE
Configuring Advanced IKE Properties
Chapter 4, Introduction to Site to Site VPN /
Configuring Site to Site VPNs
Configuring a VPN with External Gateways
Using PKI
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 and SmartDefense*
  - Chapter 13, CVP and UFP Content Security / Configuring Content Security

**Modification of IDS 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 SmartDefense 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 SmartDefense IDS capability is provided in:

- *Firewall and SmartDefense*
  - Chapter 7, SmartDefense / The SmartDefense Solution for Active Defense

Loading of SmartDefense Update files and manual definition of attack signature patterns (based on Check Point advisories) is described in:

- *CC Evaluated Configuration Administration Guide*
  - CHAPTER 13, SmartDefense Updates
Enabling or disabling Security Policy implied rules

An overview of the Implied Rules capability is provided in:

*Firewall and SmartDefense*
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 SmartCenter Server and enforcement modules is based on the Secure Internal Communications (SIC) facility. SIC certificates are issued by the Internal CA (ICA) on the SmartCenter Server, and distributed to enforcement modules.

Initial trust establishment between the enforcement module and the SmartCenter Server consists of entering an Activation key during enforcement module installation, and entering the same Activation Key in SmartDashboard.

The trust establishment process is described in:

*SmartCenter*
Chapter 1, *SmartCenter Overview / Securing Channels of Communication between Internal Components (SIC)*

*CC Evaluated Configuration Installation Guide*
CHAPTER 6, *NGX R65 Fresh Installation / Installing the Enforcement Module*
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 and SmartDefense*
  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*

*CC Evaluated Configuration Administration Guide*
  CHAPTER 8, *Site to Site VPNs*
  CHAPTER 9, *Remote Access VPN*
**User management**

User management is described in:

*SmartCenter*
Chapter 1, *SmartCenter Overview / Managing Users in SmartDashboard*

*Firewall and SmartDefense*
Chapter 2, *Authentication / Configuring 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:

*SmartCenter*
Chapter 1, *SmartCenter Overview / Managing Objects in SmartDashboard*

*CC Evaluated Configuration Administration Guide*
CHAPTER 4, *Creating the Security Policy / Defining Basic 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 enforcement modules
Log file management is described in:

*SmartCenter*
Chapter 5, *SmartView Tracker / Tracking Configuration / Maintenance*

Old log files on the SmartCenter 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 Basic Objects*

**Exporting log records to a file**

Exporting log records to a file:

*SmartCenter*
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*

*SmartCenter*
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 Gateways / 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 SmartCenter Server and enforcement modules. See:
   CC Evaluated Configuration Administration Guide
   CHAPTER 11, Monitoring System Status

   SmartView Monitor
   Chapter 5, Monitoring Gateways /
      Gateway Statuses
      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 / Alert Dialog

CC Evaluated Configuration Administration Guide
CHAPTER 11, Monitoring System Status / SmartView Monitor / Alerts
THIRD PARTY TRADEMARKS AND COPYRIGHTS

Entrust is a registered trademark of Entrust Technologies, Inc. in the United States and other countries. Entrust’s logos and Entrust product and service names are also trademarks of Entrust Technologies, Inc. Entrust Technologies Limited is a wholly owned subsidiary of Entrust Technologies, Inc. FireWall-1 and SecuRemote incorporate certificate management technology from Entrust.

Verisign is a trademark of Verisign Inc.

The following statements refer to those portions of the software copyrighted by University of Michigan. Portions of the software copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided “as is” without express or implied warranty. Copyright © Sax Software (terminal emulation only).

The following statements refer to those portions of the software copyrighted by Carnegie Mellon University.

Copyright 1997 by Carnegie Mellon University. All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The following statements refer to those portions of the software copyrighted by The Open Group.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUP 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.

The following statements refer to those portions of the software copyrighted by The OpenSSL Project. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "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 OpenSSL PROJECT 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 following statements refer to those portions of the software copyrighted by Eric Young. THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "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 AUTHOR 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. Copyright © 1998 The Open Group.

The following statements refer to those portions of the software copyrighted by Jean-loup Gailly and Mark Adler Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler. This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

The following statements refer to those portions of the software copyrighted by the Gnu Public License. This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

The following statements refer to those portions of the software copyrighted by Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 2001, 2002 Exapt maintainers. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright
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, 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, 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.

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.