Check Point
SOFTWARE TECHNOLOGIES LTD.

26 June 2018

SECURITY MANAGEMENT

R80.20.M1

Administration Guide

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page https://www.checkpoint.com/products-solutions/certified-check-point-solutions/.

Check Point R80.20.M1

For more about this release, see the R80.20.M1 home page http://supportcontent.checkpoint.com/solutions?id=sk123473.

Latest Version of this Document

Open the latest version of this document in a Web browser https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_SecurityManagement_AdminGuide/html_frameset.htm.

Download the latest version of this document in PDF format http://supportcontent.checkpoint.com/documentation_download?ID=60447.

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Security Management R80.20.M1 Administration Guide.

Revision History

Date	Description
26 June 2018	First release of this document

Contents

Terms

Administrator

A SmartConsole user with permissions to manage Check Point security products and the network environment.

DAIP Gateway

A Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway where the IP address of the external interface is assigned dynamically by the ISP.

Database

The Check Point database includes all objects, including network objects, users, services, servers, and protection profiles.

External Users

Users defined on external servers. External users are not defined in the Security Management Server database or on an LDAP server. External user profiles tell the system how to identify and authenticate externally defined users.

Identity Awareness

Lets you enforce network access and audit data based on network location, the identity of the user, and the identity of the computer.

LDAP

Lightweight Directory Access Protocol. An open industry standard for user and device data storage and directory-access.

LDAP Groups

Groups of users defined on an LDAP account unit.

Log Server

Physical server that hosts Check Point product log files.

Management Server

A Security Management Server or a Multi-Domain Server.

Package

Group of files, and data about those files, delivered as one software archive (usually TGZ or RPM), for distribution and installation.

Permissions Profile

A set of access, and feature-based roles for SmartConsole administrators.

Policy

A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

Rule Base

The database that contains the rules in a security policy and defines the sequence, in which they are enforced.

Security Gateway

A Check Point computer that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server

A Check Point computer that runs Check Point software to manage the objects and policies in Check Point environment.

SIC

Secure Internal Communication. The process by which networking components authenticate over SSL between themselves and the Security Management Server (as the (ICA) Internal Certificate Authority), for secure communication. The Security Management Server issues a certificate and components use the certificate to validate the identity of others.

SmartConsole

A Check Point GUI application used to manage security policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment and each domain.

SmartDashboard

A legacy Check Point GUI client used to create and manage the security policy in R77.30 and below.

Software Blade

A software blade is a security solution based on specific business needs.

Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

User Database

Check Point internal database that contains all users defined and managed in SmartConsole.

User Groups

Named groups of users with related responsibilities.

User Template

Property set that defines a type of user on which a security policy will be enforced.

Users

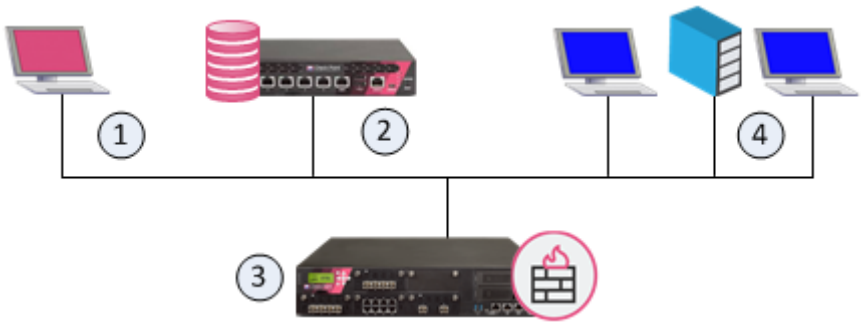
Personnel authorized to use network resources and applications.

Welcome

Check Point offers effective Security Management solutions to help you keep up with constantly growing needs and challenges of your organizational network. This Administration Guide focuses on the basic Security Management Server deployment.

If you are interested in deployments for organizations with multiple sites, refer to the *R80.20.M1 Multi-Domain Security Management Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_Multi-DomainSecurityManagement_AdminGuide/html_frameset.htm.

These are the basic components of Check Point security architecture.



Item	Description
1	SmartConsole - Check Point Graphical User Interface for connection to and management of Security Management Servers.
2	Security Management Server - Manages Security Gateways with defined security policies and monitors security events on the network.
3	Security Gateway - Placed at the perimeter of the network topology, to protect your environment through enforcement of the security policies.
4	Your environment to protect.

Getting Started

In This Section:

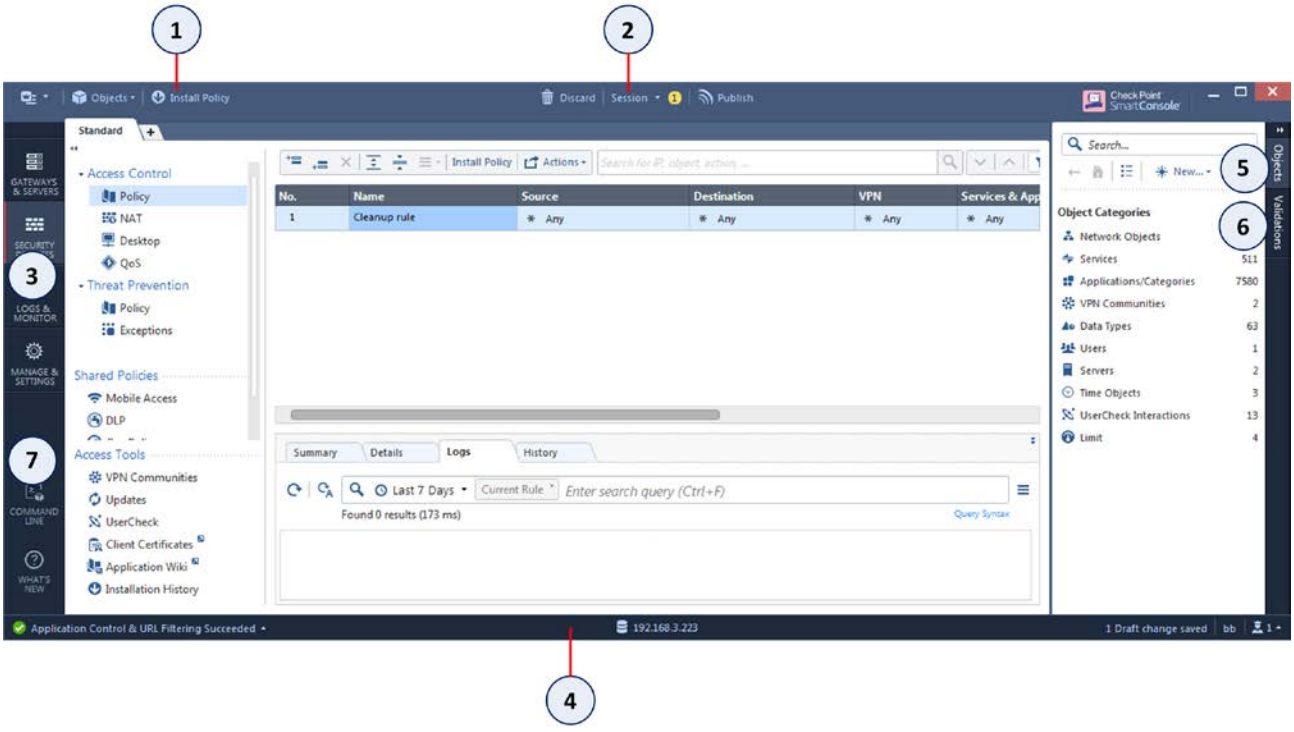
Before you begin deploying a Check Point security solution, familiarize yourself with:

- Check Point SmartConsole
- Basic setup of a Check Point Security Management Server
- Basic setup of Check Point Security Gateways
- Administrative task delegation
- Security management in a non-GUI environment

Understanding SmartConsole

Check Point SmartConsole makes it easy to manage security for complex networks. Before you start to configure your cyber security environment and policies, become familiar with Check Point SmartConsole.

SmartConsole

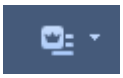


Item	Description
1	Global Toolbar
2	Session Management Toolbar
3	Navigation Toolbar
4	System Information Area

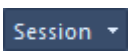
Item	Description
5	Objects Bar (F11)
6	Validations pane
7	Command line interface button

SmartConsole Toolbars

Global Toolbar (top of SmartConsole)

	Description
	The main SmartConsole Menu. When SmartConsole is connected to a Security Management Server, this includes: • Manage policies and layers • Open Object Explorer • New object (opens menu to create a new object) • Publish session • Discard session • Session details • Install policy • Verify Access Control Policy • Install Database • Uninstall Threat Prevention policy • Management High Availability • Manage Licenses and Packages • Global Properties • View (opens menu to select a View to open)
	Create new objects or open the Object Explorer
	Install policy on managed gateways

Session Management Toolbar (top of SmartConsole)

	Description
	Discard changes made during the session
	Enter session details and see the number of changes made in the session.
	Publish changes, to make them visible to other administrators, and ready to install on gateways. **Note** - When the policy is installed, published changes are installed on the gateways and enforced.

Navigation Toolbar (left side of SmartConsole)

	Keyboard Shortcut	Description
	Ctrl+1	Gateways & Servers configuration view: • Manage Security Gateways • Activate Software Blades • Add, edit, or delete gateways and clusters (including virtual clusters) • Run scripts • Backup and restore gateways • Open a command line interface on the gateway • View gateway status
	Ctrl+2	Security Policies Access Control view: • Manage Access Control: Content Awareness, VPN, Application & URL Filtering, and Mobile Access • Edit multiple policies at the same time • Add, edit, or delete NAT rules • Use the Access Tools Security Policies Threat Prevention view: • Manage Threat Prevention: IPS, Anti-Bot, Anti-Virus, Threat Emulation • Edit the unified threat Rule Base • Configure threat profiles • Add, edit, or delete exceptions and exception groups • Use the Threat Tools Shared Policies Views: • Manage Mobile Access, DLP, Geo Policy and inspection Settings
	Ctrl+3	Logs & Monitor view: • See high level graphs and plots • Search through logs • Schedule customized reports • Monitor gateways • See compliance information

	Keyboard Shortcut	Description
	Ctrl+4	Manage & Settings view - review and configure the Security Management Server settings: • Administrators • Permissions profiles • Trusted clients • Administrator sessions, and session settings • Blades • Revisions • Preferences • Sync with User Center

Command Line Interface Button (left bottom corner of SmartConsole)

	Keyboard Shortcut	Description
	F9	Open a command line interface for management scripting and API

Objects Bar (right side of SmartConsole)

	Description
Objects	Manage security and network objects

Validations Pane (right side of SmartConsole)

	Description
Validations	See validation errors

System Information Area (bottom of SmartConsole)

	Description
Task List	See management tasks in progress and expand to see recent tasks
Server Details	See the IP address of the server to which SmartConsole is connected. If Management High Availability is configured, click to see the details.
Session Status	See the number of changes made in the session and the session status.
Connected administrators	See connected administrators: Yourself and others.

Search Engine

In each view you can search the Security Management Server database for information relevant to the view. For example:

- Gateway, by name or IP address
- Access Control rule
- NAT rule
- Threat Prevention profile
- Specific threat or a threat category
- Object tags

IP Search

You can run an advanced search for an IP address, network, or port. It returns direct and indirect matches for your search criteria.

- IP address: xxx.xxx.xxx.xxx
- Network: xxx.xxx.0.0/16 or xxx.xxx
- Port: svc:<xxx>

These are the different IP search modes:

- **General –** (Default). Returns direct matched results and indirect results in IP ranges, networks, groups, groups with exclusion, and rules that contain these objects.
- **Packet** – Matches rules as if a packet with your IP address arrives at the gateway.

General IP Search

This is the default search mode. Use it to search in Rule Bases and in objects. If you enter a string that is not a valid IP or network, the search engine treats it as text.

When you enter a valid IP address or network, an advanced search is done and on these objects and rules:

- Objects that have the IP address as a text value for example, in a comment
- Objects that have an IP address property (direct results)
- Groups, networks, and address ranges that contain objects with the text value or address value
- Rules that contain those objects

Packet Search

A Packet Search matches rules as if a packet with your IP address arrives at the gateway. It matches rules that have:

- The IP address in a column of the rule
- "Any"
- A Group-with-exclusion or negated field with the IP address in its declaration

To run a Packet Search:

1. Click the search box.
   The search window opens.
2. Click **Packet** or enter: "mode:Packet"
3. To search a specific rule column, enter: *ColumnName:Criteria*

Rule Base Results

When you enter search criteria and view the matched results, the value that matched the criteria in a rule is highlighted.

If there is...	This is highlighted
A direct match on an object name or on textual columns	Only the specific matched characters
A direct match on object properties	The entire object name
A negated column	The negated label
A match on "Any"	"Any"

Known Limitation:

- Packet search does not support IPv6.

Access and Threat Tools

The **Access Tools** section in the **Security Policies Access Control** view and the **Threat Tools** section in the **Security Policies Threat Prevention** view give you more management and data collection tools.

Access Tools in the **Security Policies Access Control** view:

Tool	Description
VPN Communities	Create, edit, or delete VPN Communities.
Updates	Update the Application & URL Filtering database, schedule updates, and configure updates.
UserCheck	Configure UserCheck interaction objects for Access Control policy actions.
Client Certificates	Create and distribute client certificates that allow users to authenticate to the Gateway from handheld devices.
Application Wiki	Browse to the Check Point AppWiki. Search and filter the Web 2.0 Applications Database, to use Check Point security research in your policy rules for actions on applications, apps, and widgets.

Tool	Description
Installation History	See the Policy installation history for each Gateway, and who made the changes. See the revisions that were made during each installation, and who made them. Install a specific version of the Policy.

Threat Tools in the **Security Policies Threat Prevention** view:

Tool	Description
Profiles	Create, edit, or delete profiles.
IPS Protections	Edit IPS protections per profile.
Protections	See statistics on different protections
Whitelist Files	Configure Whitelist Files list
Indicators	Configure indicators of malicious activity and how to handle it
Updates	Configure updates to the Malware database, Threat Emulation engine and images, and the IPS database.
UserCheck	Configure UserCheck interaction objects for Threat Prevention policy actions.
Threat Wiki	Browse to the Check Point ThreatWiki. Search and filter Check Point's Malware Database, to use Check Point security research to block malware before it enters your environment, and to best respond if it does get in.
Installation History	See the Policy installation history for each Gateway, and who made the changes. See the revisions that were made during each installation, and who made them. Install a specific version of the Policy.

Shared Policies

The **Shared Policies** section in the **Security Policies** shows the policies that are not in a Policy package. They are shared between all Policy packages.

Shared policies are installed with the Access Control Policy.

Software Blade	Description
Mobile Access	Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP	Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy	Create a policy for traffic to or from specific geographical or political locations.

Software Blade	Description
HTTPS Inspection	The HTTPS Policy allows the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol. The HTTPS Policy shows if HTTPS inspection is enabled on one or more Gateways. To learn more about HTTPS Inspection, see the *R80.10 Next Generation Security Gateway Guide*. http://downloads.checkpoint.com/dc/download.htm?ID=54806
Inspection Settings	You can configure Inspection Settings (on page 258) for the Firewall: • Deep packet inspection settings • Protocol parsing inspection settings • VoIP packet inspection settings

API Command Line Interface

You can also configure objects and rules through the API command line interface, which you can access from SmartConsole.

Click to open the command line interface.

Click to open the API reference (in the command line interface).

Use the Command Line Reference to learn about **Session management** commands, **Host** commands, **Network** commands, and **Rule** commands.

In addition to the command line interface, you can create and run API scripts to manage configuration and operations on the Security Management Server ("Managing Security through API and CLI" on page 23).

See the or CLI commands

Connecting to the Security Management Server through SmartConsole

To log in to a Security Management Server through Check Point SmartConsole, you must have an administrator account configured on the Security Management Server. When installing the Security Management Server, you create one administrator in the First Time Configuration Wizard. After that, you can create additional administrators accounts with SmartConsole, or using the Gaia Portal.

To log in to the Security Management Server through SmartConsole:

1. Launch the SmartConsole application.
2. Enter your administrator authentication credentials. These can be a *username*, or a *certificate file*, or a *CAPI certificate*.

   Logging in with a username:

   - Enter the **Username** and **Password**.

   Logging in with a certificate file:

   - From the drop-down list, select **Certificate File**.

- Browse to the file.
- Enter the password of the certificate file.

Logging in with a certificate in the CAPI repository:

- From the drop-down list, select **CAPI Certificate**.
- Select the certificate from drop-down list.

3. Enter the name or the IP address of the Security Management Server.
4. Click **Login**.

   The SmartConsole authenticates the Security Management Server. The first time you connect, SmartConsole shows the fingerprint.
5. Confirm the fingerprint.

The fingerprint and the IP address of the Security Management Server are saved to the user settings in Windows.

Setting Up for Security Management

To start setting up your security environment, configure the Security Management Server and the Security Gateways. The Security Gateways enforce the security policy that you define on the Security Management Server.

To configure the Security Management Server in SmartConsole:

1. In the **Gateways & Servers** view, find the Security Management Server object.

   You can search for it by name or IP address in the **Search** box at the top of the view.

   When you select the Security Management Server object, the **Summary** tab at the bottom of the pane shows the Software Blades that are enabled on it.
2. Open the object properties window, and enable the Management Software Blades, as necessary:
   - **Network Policy Management** - Manage a comprehensive security policy, unified for all security functionalities. This is automatically enabled.
   - **Endpoint Policy Management** - Manage security and data on end-user computers and hand-held devices. Enable this Software Blade if you have or will install an Endpoint Security Management Server.
   - **Logging & Status** - Monitor security events and status of gateways, VPNs, users, and more, with advanced visuals and data management features.
   - **Identity Logging** - Add user identities, and data of their computers and devices, from Active Directory domains, to log entries.
   - **User Directory** - Populate your security scope with user accounts from the LDAP servers in your environment.
   - **Compliance** - Optimize your security settings and comply with regulatory requirements
   - **SmartEvent** - Manage and correlate security events in real-time.

To configure the Security Gateways in SmartConsole:

1. From the navigation toolbar, select **Gateways & Servers**.
2. Click **New**, and select **Gateway**.
3. In the **Check Point Security Gateway Creation** window that opens, select a configuration mode:
   - **Wizard Mode** - run the configuration wizard
   - **Classic Mode** - configure the gateway in classic mode ("Creating a New Security Gateway" on page 43)

Setting up for Team Work

As an administrator, you can delegate tasks, such as defining objects and users, to other administrators. Make sure to create administrator accounts ("Managing Administrator Accounts" on page 26) with the privileges that are required to accomplish those tasks.

If you are the only administrator, we recommend that you create a second administrator account with Read Only permissions, which is useful for troubleshooting, consultation, or auditing.

Managing Security through API and CLI

You can configure and control the Security Management Server with the new command line tools and through web services. You must first configure the API server.

The API server runs scripts that automate daily tasks and integrate the Check Point solutions with third party systems such as virtualization servers, ticketing systems, and change management systems.

You can use these tools to run API scripts on the Security Management Server:

- Standalone management tool, included with SmartConsole. You can copy this tool to Windows or Gaia computers.
  - `mgmt_cli.exe` (Windows)
  - `mgmt_cli` (Gaia)
- Web Services API that allows communication and data exchange between the clients and the Security Management Server through the HTTP protocol. It also lets other Check Point processes communicate with the management server through the HTTPS protocol.

All API clients use the same port as the Gaia portal.

To learn more about the management APIs, to see code samples, and to take advantage of user forums, see the **Developers Network** section of CheckMates https://community.checkpoint.com.

And visit the Online API Reference Guide https://sc1.checkpoint.com/documents/latest/APIs/index.html.

Configuring the API Server

To configure the API Server:

1. In SmartConsole, go to **Manage & Settings** > **Blades**.
2. In the **Management API** section, click **Advanced Settings**.
   The **Management API Settings** window opens.
3. Configure the **Startup Settings** and the **Access Settings**.

Management API Settings

- **Startup Settings**
  - Select **Automatic start** to automatically start the API server when the Security Management Server starts.

    In these environments, **Automatic start** is selected by default:

    - Distributed Security Management Servers (without gateway functionality) with at least 4GB of RAM
    - Standalone Security Management Servers (with gateway functionality) with at least 8GB of RAM

  In other environments, to reduce the memory consumption on the management server, **Automatic start** is not selected by default.
- **Access Settings**

  Configure IP addresses from which the API server accepts requests:
  - **Management server only** (default) - API server will accept scripts and web service requests only from the Security Management Server. You must open a command line interface on the server and use the `mgmt_cli` utility to send API requests.
  - **All IP addresses that can be used for GUI clients** - API server will accept scripts and web service requests from the same devices that are allowed access to the Security Management Server.
  - **All IP addresses** - API server will accept scripts and web-service requests from any device.

To apply changes, you must publish the session, and run the `api restart` command on the Security Management Server.

Planning Security Management

After installing the Security Management Server and the Security Gateways, you can continue with cyber security configuration for your environment.

Define your organization's topology

Network topology consists of network components, both physical and logical, such as physical and virtual Security Gateways, hosts, hand-held devices, CA servers, third-party servers, services, resources, networks, address ranges, and groups. Each of these components corresponds to an object in your Check Point security management configuration. Configure those objects ("Network Object Types" on page 55) in SmartConsole.

Define users and user groups that your security environment protects

You can add users ("Creating, Modifying, Removing User Accounts" on page 215) and groups ("Managing User Groups" on page 218) to the database manually, through LDAP and User Directory (on page 218), or with the help of Active Directory ("Microsoft Active Directory" on page 237).

Define access rules for protection of your organization's resources

Configure access rules and group them in policies that are enforced on the Security Gateways. You can define access policies ("Managing Policies" on page 68) based on traffic, applications, Web sites, and data. Set up preventative actions against known threats with Check Point Anti-Virus and Anti-Malware. Educate users about the validity and security of the operations they attempt with the help of UserCheck. Track network traffic and events through logging and monitoring.

Enforce access policies

Configure the Security Gateways. Make sure to activate the appropriate Software Blades. Then, install your policies on the Security Gateways.

Managing Administrator Accounts

In This Section:

Creating and Changing an Administrator Account

To successfully manage security for a large network, we recommend that you first set up your administrative team, and delegate tasks.

We recommend that you create administrator accounts in SmartConsole, with the procedure below or with the First Time Configuration Wizard.

If you create it through the SmartConsole, you can choose one of these authentication methods:

- Check Point Password (on page 210)
- OS Password (see "Operating System Password" on page 210)
- RADIUS (on page 210)
- SecurID (on page 211)
- TACACS (on page 211)

To create an administrator account using SmartConsole:

1. Click **Manage & Settings > Permissions and Administrators**.
   The **Administrators** pane shows by default.
2. Click **New Administrator**.
   The **New Administrators** window opens.
3. Enter a unique name for the administrator account.
   Note - This parameter is case-sensitive.
4. Set the Authentication Method, or create a certificate, or the two of them.
   Note - If you do not do this, the administrator will not be able to log in to SmartConsole.
   To define an Authentication Method:
   In the **Authentication Method** section, select a method and follow the instructions in *Configuring Authentication Methods for Administrators* (on page 39).

To create a Certificate - If you want to use a certificate to log in:

In the **Certificate Information** section, click **Create**, and follow the instructions in *Configuring Certificates for Administrators* ("Creating a Certificate for Logging in to SmartConsole" on page 27).

5. Select a **Permissions** profile for this administrator, or create a new one ("Changing and Creating Permission Profiles" on page 29).
6. Set the account **Expiration** date:
   - For a permanent administrator - select **Never**
   - For a temporary administrator - select an **Expire At** date from the calendar

   The default expiration date shows, as defined in the Default Expiration Settings ("Configuring Default Expiration Settings for Users" on page 217). After the expiration date, the account is no longer authorized to access network resources and applications.
7. **Optional**: Configure **Additional Info - Contact Details**, **Email** and **Phone Number** of the administrator.
8. Click **OK**.

To change an existing administrator account:

1. Click **Manage & Settings** > **Permissions and Administrators**.
2. Double-click an administrator account.

   The **Administrators** properties window opens.

Creating an administrator with cpconfig

We do not recommend creating an administrator with `cpconfig`, the Check Point Configuration Tool. Use it only if there is no access to SmartConsole or the Gaia Portal. If you use `cpconfig` to create an administrator:

- You must restart Check Point Services to activate the administrator.
- It does not show the other administrators
- Check Point Password is automatically configured as the authentication method.

Creating a Certificate for Logging in to SmartConsole

When you define an administrator, you must configure the authentication credentials for the administrator.

The authentication credentials for the administrator can be one of the supported authentication methods, or a certificate, or the two of them.

You can create a certificate file in SmartConsole. The administrator can use this file to log in to SmartConsole using the *Certificate File* option. The administrator must provide the password for the certificate file.

You can import the certificate file to the CryptoAPI (CAPI) certificate repository on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole using the *CAPI Certificate* option. The SmartConsole administrator does not need to provide a password.

To create a certificate file:

1. In the **New Administrator** window, in the **Certificate Information** section, click **Create**.
2. Enter a password.
3. Click **OK**.
4. Save the certificate file to a secure location on the SmartConsole computer.

The certificate file is in the PKCS #12 format, and has a `.p12` extension.

Note - Give the certificate file and the password to the SmartConsole administrators. The administrator must provide this password when logging in to SmartConsole with the **Certificate File** option.

To Import the certificate file to the CAPI repository:

1. On the Microsoft Windows SmartConsole computer, double-click the certificate file.
2. Follow the instructions.

Configuring Default Expiration for Administrators

If you want to use the same expiration settings for multiple accounts, you can set the default expiration for administrator accounts. You can also choose to show notifications about the approaching expiration date at the time when an administrator logs into SmartConsole or one of the SmartConsole clients. The remaining number of days, during which the account will be alive, shows in the status bar.

To configure the default expiration settings:

1. Click **Manage & Settings > Permissions and Administrators > Advanced**.
2. Click **Advanced**.
3. In the **Default Expiration Date** section, select a setting:
   - **Never expires**
   - **Expire at** - Select the expiration date from the calendar control
   - **Expire after** - Enter the number of days, months, or years (from the day the account is made) before administrator accounts expire
4. In the **Expiration notifications** section, select **Show 'about to expire' indication in administrators view** and select the number of **days in advance** to show the message about the approaching expiration date.
5. Click **Publish**.

Setting SmartConsole Timeout

Use the SmartConsole in a secure manner, and enforce secure usage for all administrators. Setting a SmartConsole timeout is a basic requirement for secure usage. When an administrator is not using the SmartConsole, it logs out.

To set the SmartConsole timeout:

1. Click **Manage & Settings**.
2. Select **Permissions & Administrators** > **Advanced.**
3. In the **Idle Timeout area**, select **Perform logout after being idle**.

4. Enter a number of minutes.

   When a SmartConsole is idle after this number of minutes, the SmartConsole automatically logs out the connected administrator, but all changes are preserved.

Deleting an Administrator

To make sure your environment is secure, it is best practice to delete administrator accounts when personnel leave or transfer.

To remove an administrator account:

1. Click **Manage & Settings** > **Permissions and Administrators**.

   The **Administrators** pane shows by default.
2. Select an administrator account and click **Delete**.
3. Click **Yes** in the confirmation window that opens.

Revoking Administrator Certificate

If an administrator that authenticates through a certificate is temporarily unable to fulfill administrator duties, you can revoke the certificate for the account. The administrator account remains, but no one can authenticate to the Security Management Server with the certificate. However, if the account has an additional authentication method (a password, for example), that method can be used to authenticate to the account.

To revoke an administrator certificate:

1. Click **Manage & Settings** > **Permissions and Administrators**.
2. Select an administrator account and click **Edit**.
3. In **General** > **Authentication**, click **Revoke**.

Assigning Permission Profiles to Administrators

A permission profile is a predefined set of Security Management Server and SmartConsole administrative permissions that you can assign to administrators. You can assign a permission profile to more than one administrator. Only Security Management Server administrators with the *Manage Administrators* permission in the profile can create and manage permission profiles.

To learn about permission profiles for Multi-Domain Security Management administrators, see the *R80.20.M1 Multi-Domain Security Management Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_Multi-DomainSecurityManagement_AdminGuide/html_frameset.htm.

Changing and Creating Permission Profiles

Administrators with Super User permissions can edit, create, or delete permission profiles.

These are the predefined, default permission profiles. You cannot change or delete the default permission profiles. You can clone them, and change the clones:

- **Read Only All** - Full Read Permissions. No Write permissions.

- **Read Write All** - Full Read and Write Permissions.
- **Super User** - Full Read and Write Permissions, including managing administrators and sessions.

To change the permission profile of an administrator:

1. Click **Manage & Settings** > **Permissions and Administrators**.
2. Double-click the administrator account.

   The **Administrators** properties window opens.
3. In the **Permissions** section, select another **Permission Profile** from the list.
4. Click **OK**.

To change a permission profile:

1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Permission Profiles**.
2. Double-click the profile to change.
3. In the **Profile** configuration window that opens, change the settings as needed.
4. Click **Close**.

To create a new permission profile:

1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Permission Profiles**.
2. Click **New Profile**.

   The **New Profile** window opens.
3. Enter a unique name for the profile.
4. Select a profile type:
   - **Read/Write All** - Administrators can make changes to all features
   - **Auditor (Read Only All)** - Administrators can see all information but cannot make changes
   - **Customized** - Configure custom settings ("Configuring Customized Permissions" on page 31)
5. Click **OK**.

To delete a permission profile:

1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Permission Profiles**.
2. Select a profile and click **Delete**.

   You cannot delete a profile that is assigned to an administrator. To see which administrators use a profile, in the error message, click **Where Used**.

   If the profile is not assigned to administrators, a confirmation window opens.
3. Click **Yes** to confirm.

Configuring Customized Permissions

Configure administrator permissions for **Gateways**, **Access Control**, **Threat Prevention**, **Others**, **Monitoring and Logging**, **Events and Reports**, **Management**. For each resource, define if administrators that are configured with this profile can configure the feature or only see it.

Permissions:

- **Selected** - The administrator has this feature.
- **Not selected** - The administrator does not have this feature.
  Note - If you cannot clear a feature selection, the administrator access to it is mandatory.

Some features have **Read** and **Write** Options. If the feature is selected:

- **Read** - The administrator has the feature but cannot make changes.
- **Write** - The administrator has the feature and can make changes.

To configure customized permissions:

1. In the **Profile** object, in the **Overview > Permissions** section, select **Customized**.
2. Configure permissions in these pages of the **Profile** object:
   - **Gateways -** configure the **Provisioning** and the **Scripts** permissions.
   - **Access Control** - configure Access Control Policy permissions ("Configuring Permissions for Access Control and Threat Prevention" on page 32).
   - **Threat Prevention** - configure Threat Prevention Policy permissions ("Configuring Permissions for Access Control and Threat Prevention" on page 32).
   - **Others** - configure permissions for **Common Objects**, user databases, **HTTPS Inspection** features, and **Client Certificates**.
   - **Monitoring and Logging** - configure permissions to generate and see logs and to use monitoring features ("Configuring Permissions for Monitoring, Logging, Events, and Reports" on page 33).
   - **Events and Reports** - configure permissions for SmartEvent features ("Configuring Permissions for Monitoring, Logging, Events, and Reports" on page 33).
3. In the **Management** section, configure this profile with permissions to:
   - **Manage Administrators -** Manage other administrator accounts.
   - **Manage Sessions -** Lets the administrator configure the session management settings (single or multiple sessions)
   - the session mode for single or multiple sessions
   - **High Availability Operations -**Configure and work with High Availability.
   - **Management API Login -** Log in with the management API.
4. Click **OK**.

Configuring Permissions for Access Control Layers

You can simplify the management of the Access Control Policy by delegating ownership of different Layers to different administrators.

To do this, assign a permission profile to the Layer. The permission Profile must have this permission: **Edit Layer by the selected profiles in a layer editor**.

An administrator that has a permission profile with this permission can manage the Layer.

Workflow:

1. Give Layer permissions to an administrator profile.
2. Assign the permission profile to the Layer.

To give Layer permissions to an administrator profile:

1. In the **Profile** object, in the **Access Control > Policy** section, select **Edit Layer by the selected profiles in a layer editor**.
2. Click **OK**.

To assign a permission profile to a Layer:

1. In SmartConsole, click **Menu** > **Manage policies and layers**.
2. In the left pane, click **Layers**.
3. Select a Layer.
4. Click **Edit**.
5. In the left pane, select **Permissions**.
6. Click **+**
7. Select a profile with Layer permissions.
8. Click **OK**.
9. Click **Close**.
10. **Publish** the session.

Configuring Permissions for Access Control and Threat Prevention

In the **Profile** object, select the features and the Read or Write administrator permissions for them.

Access Control

To edit a Layer, a user must have permissions for all Software Blades in the Layer.

- **Actions**
  - **Install Policy** - Install the Access Control Policy on Security Gateways.
  - **Application & URL Filtering Update** - Download and install new packages of applications and websites, to use in access rules.

Threat Prevention

- **Actions**
  - **Install Policy** - Install the Threat Prevention Policy on Security Gateways.
  - **IPS Update -** Download and install new packages for IPS protections.

Configuring Permissions for Monitoring, Logging, Events, and Reports

In the **Profile** object, select the features and the Read or Write administrator permissions for them.

Monitoring and Logging Features

These are *some* of the available features:

- **Monitoring**
- **Management Logs**
- **Track Logs**
- **Application and URL Filtering Logs**

Events and Reports Features

These are the permissions for SmartEvent:

- **SmartEvent**
  - **Events** - views in SmartConsole > Logs & Monitor
  - **Policy** - Events correlation on the **Policy** tab
  - **Reports** - in SmartConsole > Logs & Monitor
- **SmartEvent Application & URL Filtering reports only**

Defining Trusted Clients

By default, any authenticated administrator can connect to the Security Management Server from any computer. To limit the access to a specified list of hosts, can configure **Trusted Clients**. You can configure **Trusted Clients** in these ways:

- **Any** - All hosts (default)
- **IPv4 Address** - A single host with specified IPv4 address
- **IPv4 Address Range** - Hosts with IPv4 addresses in the specified range
- **IPv4 Netmask** - Hosts with IPv4 addresses in the subnet defined by the specified IPv4 address and netmask
- **IPv6 Address** - A single host with specified IPv6 address
- **IPv6 Address Range** - Hosts with IPv6 addresses in the specified range
- **IPv6 Netmask** - Hosts with IPv6 addresses in the subnet defined by the specified IPv6 address and netmask
- **Name** - A host with the specified name
- **Wild cards (IP only)** - Hosts with IP addresses described by the specified regular expression

Configuring Trusted Clients

Administrators with Super User permissions can add, edit, or delete trusted clients.

To add a new trusted client:

1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Trusted Clients**.
2. Click **New**.
   The **New Trusted Client** window opens.
3. Enter a unique name for the client.
4. Select a client type and configure corresponding values:
   - **Any** - No values to configure
   - **IPv4 Address** - Enter an IPv4 address of a host
   - **IPv4 Address Range** - Enter the first and the last address of an IPv4 address range
   - **IPv4 Netmask** - Enter the IPv4 address and the netmask
   - **IPv6 Address** - Enter an IPv6 address of a host
   - **IPv6 Address Range** - Enter the first and the last address of an IPv6 address range
   - **IPv6 Netmask** - Enter the IPv6 address and the netmask
   - **Name** - Enter a host name
   - **Wild cards (IP only)** - Enter a regular expression that describes a set of IP addresses
5. Click **OK**.

To change trusted client settings:

1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Trusted Clients**.
2. Double-click the client you want to edit.
3. In the **Trusted Client** configuration window that opens, change the settings as needed.
4. Click **OK**.

To delete a trusted client:

1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Trusted Clients**.
2. Select a trusted client and click **Delete**.
   The confirmation window opens.
3. Click **Yes** to confirm.

Restricting Administrator Login Attempts

For administrators that login to the Security Management Server using a Check Point password, you can configure these login restrictions:

- The number of login attempts before SmartConsole automatically locks an administrator.
- The number of minutes before SmartConsole unlocks the administrator's account after it was locked.

To configure login restrictions:

1. Go to the **Manage & Settings** view or to the **Multi-Domain** view.
2. Go to **Permissions & Administrators** > **Advanced** > **Login Restrictions**.

Note - these restrictions apply *only* to administrators that authenticate to the Security Management Server using a Check Point password.

Unlocking Administrators

An administrator who has the **Manage Administrators** permission can unlock another administrator *if the locked administrator authenticates to the Security Management Server using a Check Point password*.

To unlock an administrator:

1. Go to the **Manage & Settings** view or to the **Multi-Domain** view.
2. Right-click the locked administrator and select **Unlock Administrator**.

Or:

Use the unlock administrator API command https://sc1.checkpoint.com/documents/R80/APIs/#gui-cli/unlock-administrator.

Note - the **Unlock Administrator** feature does *not* apply to administrators using other authentication methods.

Session Flow for Administrators

In SmartConsole, administrators work with sessions. A session is created each time an administrator logs into SmartConsole. Changes made in the session are saved automatically. These changes are private and available only to the administrator. To avoid configuration conflicts, other administrators see a lock icon on objects and rules that are being edited in other sessions.

Administrators can publish or discard their private changes. To include private changes in the policy installation, sessions containing these private changes must be published. This is also true if you want to make your private changes available to other administrators. Unpublished changes from other sessions are not included in the policy installation.

Before you publish a session, we recommend that you give the session a name and add a brief description that documents the work process.

Publishing a Session

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, or the use of objects that are not valid in the Rule Base. Make sure you correct these errors before publishing.

To publish a session:

On the **SmartConsole** toolbar, click **Publish**. When a session is published, a new database version is created and shows in the list of database revisions.

To add a name or description to a session:

1. In the **SmartConsole** toolbar, click **Session**.
   The **Session Details** window opens.
2. Enter a name for the database version.
3. Enter a description.
4. Click **OK**.

To discard a session:

In the **SmartConsole** toolbar, click **Discard**.

Working in SmartConsole Session View

The Session view shows all unpublished sessions in the system. The view shows the sessions of the current administrator, sessions of other administrators and sessions from other applications. The columns in the view can be customized and show the session owner, name, description, connection mode, number of private changes, number of locks, application and other values.

To see session information, click **Manage & Settings > Sessions > View Sessions**.

Actions available to administrators on private sessions is determined by the **Manage Sessions** permission on their profile.

Administrators without the Manage Session permission can:	Administrators with the Manage Session Permission can:
• Publish and discard their own sessions • See sessions opened by other administrators, the number the locks they have and number of changes they have made • Take over sessions created by applications, for example sessions created by the API command line tool	• Publish and discard their own sessions • See sessions opened by other administrators, the number the locks they have and number changes they have made • **Publish & Disconnect** the private sessions of other administrators • **Disconnect & Discard** the private sessions of other administrators • **Disconnect** another administrator's private session • **Take over** sessions created by applications, for example sessions created by the API command line tool • **Take over** the private sessions of other administrators. **Note**: If you want to keep changes made in your own private session, publish these changes *before* you take over the session of another administrator. If you do not publish your changes, you will lose them. When you take over, you disconnect the other administrator's SmartConsole session. • **Publish & Disconnect** the private sessions of other administrators. The action applies to both SmartConsole sessions and command line API sessions. • **Disconnect** the private session of other administrators • **Discard & Disconnect** the private session of other administrators

Administrator's Working with Multiple Sessions

Administrators working with multiple sessions can open multiple new private sessions without publishing changes made in their current private session.

Use Case

Suppose you are making changes in a private session and are asked to solve some immediate problem. The task involves making a change and publishing it. You do not wish to publish or discard your current private session.

You open a new private session, make the change required resolve the issue, publish the change, then return to your previous private session.

To do this, you need to work with *multiple sessions*. To switch on multiple sessions, you need **The Manage Sessions** permission selected on your administrator profile.

To enable working in multiple sessions:

1. Open the relevant permission profile.
2. Make sure the **Manage Sessions** permission is selected on the **Management** page.
3. Open **SmartConsole** > **Manage & Settings** View > **Sessions** > **Advanced**.
4. Select **Each administrator can manage multiple SmartConsole sessions at the same time**.
5. **Publish** the change.

When working with *multiple sessions*, you can:

- Open and manage multiple sessions to the Security Management Server using the same administrator account
- Switch between the active session and previously saved sessions
- Publish, discard and disconnect other sessions
- Take over other sessions

The SmartConsole Session menu

After multiple sessions are enabled, the SmartConsole Session menu has these new options:

Option	Description
Edit sessions details	Lets you change the session name and description.
Create new session	**In the current window** Opens a new session in the current SmartConsole **In a new window** Opens a new session in a new SmartConsole
Recent	Shows a list of recent sessions. Selecting a session opens the session in the current SmartConsole
More	Opens the **Open Session** window that shows sessions that you previously created and saved. • Sessions shown in this window are owned by the current user in the current domain. • The **Open Session > Actions** menu has options to open a saved session in the current SmartConsole or open the session in a new SmartConsole.

The SmartConsole Session View

When multiple sessions are enabled, you can perform these additional actions:

Action	You can:
For sessions that you own	• Discard and Disconnect • Publish and Disconnect • Disconnect • Open an older session
For sessions owned by other administrators that have made private changes	• Publish and Disconnect their changes • Discard and Disconnect • Disconnect • Take over their changes
For sessions owned by other administrators that have not made private sessions	• Disconnect • Take over

Note: When working in single session, you need to publish or discard your changes before taking over another session. In multi session, you do not have to publish or discard your session before taking over the session of another administrator.

Switching between Multiple and Single Session

If the session management settings switch from multiple SmartConsole sessions to allow only a single SmartConsole session at a time:

- Administrators can still publish, discard and open sessions that they own.
- Cannot create new sessions until they have published or discarded all their unpublished sessions with private sessions
- Cannot take over the sessions of other administrators or applications (for example sessions created with API commands in the *mgmt_cli* utility) until they have published or discarded all their previously saved private sessions.

Configuring Authentication Methods for Administrators

These instructions show how to configure authentication methods for *administrators*. For *users*, see *Configuring Authentication Methods for Users* (on page 211).

For background information about the authentication methods, see *Authentication Methods for Users and Administrators* (on page 210).

Configuring Check Point Password Authentication for Administrators

These instructions show how to configure Check Point Password (on page 210) authentication for administrators.

To configure a Check Point password for a SmartConsole administrator:

1. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
2. Click **New**.

3. The **New Administrator** window opens.
4. Give the administrator a name.
5. In **Authentication method**, select *Check Point Password*.
6. Click **Set New Password**, type the **Password**, and **Confirm** it.
7. Assign a **Permission Profile**.
8. Click **OK**.
9. Click **Publish**.

Configuring OS Password Authentication for Administrators

These instructions show how to configure OS Password Authentication (see "Operating System Password" on page 210) for administrators.

To configure an OS password for a SmartConsole administrator:

1. Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
2. Click **New**.
3. The **New Administrator** window opens.
4. Give the administrator a name.
5. In **Authentication method**, select *OS Password*.
6. Assign a **Permission Profile**.
7. Click **OK**.
8. Click **Publish**.

Configuring a RADIUS Server for Administrators

These instructions show how to configure a RADIUS (on page 210) server for SmartConsole administrators. To learn how to configure a RADIUS server, refer to the vendor documentation.

To configure a RADIUS Server for a SmartConsole administrator:

1. In SmartConsole, click **Objects** > **More Object Types** > **Server** > **More** > **New RADIUS**.
2. Configure the **RADIUS Server Properties**:
   a) Give the server a **Name**. It can be any name.
   b) Click **New** and create a **New Host** with the **IP address** of the RADIUS server.
   c) Click **OK**.
   d) Make sure that this host shows in the **Host** field of the **Radius Server Properties** window.
   e) In the **Shared Secret** field, type the secret key that you defined previously on the RADIUS server.
   f) Click **OK**.
   g) Click **Publish**.
3. Add a new administrator:
   a) Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
   b) Click **New**.

      The **New Administrator** window opens.

c) Give the administrator the name that is defined on the RADIUS server.

d) Assign a **Permission Profile**.

e) In **Authentication method**, select *RADIUS*.

f) Select the **RADIUS Server** defined earlier.

g) Click **OK**.

4. Click **Publish**.

Configuring a SecurID Server for Administrators

These instructions show how to configure a SecurID (on page 211) server for SmartConsole administrators. To learn how to configure a SecurID server, refer to the vendor documentation.

To configure the Security Management Server for SecurID:

1. Connect to the Security Management Server.
2. Copy the `sdconf.rec` file to the `/var/ace/` folder
   If the folder does not exist, create the folder.
3. Give the `sdconf.rec` file full permissions. Run:
   ```
   chmod 777 sdconf.rec
   ```

To configure a SecurID Server for a SmartConsole administrator:

1. In SmartConsole, click **Objects** > **More Object Types** > **Server** > **More** > **New SecurID**.
2. Configure the **SecurID Properties**:
   a) Give the server a **Name**. It can be any name.
   b) Click **Browse** and select the `sdconf.rec` file. This must be a copy of the file that is on the Security Management Server.
   c) Click **OK**.
3. Add a new administrator:
   a) Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
   b) Click **New**.
      The **New Administrator** window opens.
   c) Give the administrator a name.
   d) Assign a **Permission Profile**.
   e) In **Authentication method**, select *SecurID*.
4. In the SmartConsole Menu, click **Install Database**.

Configuring a TACACS Server for Administrators

These instructions show how to configure a TACACS (on page 211) server for SmartConsole administrators. To learn how to configure a TACACS server, refer to the vendor documentation.

To configure a TACACS Server for a SmartConsole administrator:

1. In SmartConsole, click **Objects** > **More Object Types** > **Server** > **More** > **New TACACS**.
2. Configure the **TACACS Server Properties**:
   a) Give the server a **Name**. It can be any name.
   b) Click **New** and create a **New Host** with the **IP address** of the TACACS server.
   c) Click **OK**.
   d) Make sure that this host shows in the **Host** field of the **TACACS Server Properties** window.
   e) In the **Shared Secret** field, type the secret key that you defined previously on the TACACS server.
   f) Click **OK**.
   g) Click **Publish**.
3. Add a new administrator:
   a) Go to **Manage & Settings** > **Permissions & Administrators** > **Administrators**.
   b) Click **New**.

      The **New Administrator** window opens.
   c) Give the administrator the name that is defined on the TACACS server.
   d) Assign a **Permission Profile**.
   e) In **Authentication method**, select *TACACS*.
   f) Select the **TACACS Server** defined earlier.
   g) Click **OK**.
4. Click **Publish**.

Managing Gateways

In This Section:

Creating a New Security Gateway

A Security Gateway enforces security policies configured on the Security Management Server.

To install security policies on the Security Gateways, configure the gateway objects in SmartConsole.

To define a new Security Gateway object:

1. From the navigation toolbar, select **Gateways & Servers**.
2. Click **New**, and select **Gateway**.
   The **Check Point Security Gateway Creation** window opens.
3. Click **Classic Mode**.
   The **Check Point Gateway** properties window opens and shows the **General Properties** screen.
4. Enter the host **Name** and the **IPv4 Address** or **IPv6 Address**.
5. Click **Communication**.
   The **Trusted Communication** window opens.
6. Select a **Platform**.
7. In the **Authentication** section, enter and confirm the **One-time password**.
   If you selected **Small Office Appliance** platform, make sure **Initiate trusted communication automatically when the Gateway connects to the Security Management Server for the first time** is selected.
8. Click **Initialize** to establish trusted communication with the gateway ("Secure Internal Communication (SIC)" on page 45).
   If trust fails to establish, click **OK** to continue configuring the gateway.
9. Click **OK**.
10. The **Get Topology Results** window that opens, shows interfaces successfully configured on the gateway.
11. Click **Close**.
12. In the **Platform** section, select the **Hardware**, the **Version**, and the **OS**.
    If trust is established between the server and the gateway, click **Get** to automatically retrieve the information from the gateway.
13. Select the Software Blades to enable on the Security Gateway.
    For some of the Software Blades a first-time setup wizard will open. You can run the wizard now or later. For more on the setup wizards, see the relevant Administration Guide.

Manually Updating the Gateway Topology

As the network changes, you must update the gateway topology.

To update the gateway topology:

1. In SmartConsole, click **Gateways & Servers**.
2. Double-click the gateway object.
   The gateway property window opens.
3. Click **Network Management**.
4. Click **Get Interfaces**.
   A warning window asks if you want to overwrite the existing Topology and Anti-spoofing settings.
5. Click **Yes**.
6. The **Get Topology Results** window opens.
7. Click **Accept**.
8. Click **OK**.

Dynamically Updating the Topology

This feature is supported only for R80.20 and above gateways. Once selected, the range of IP addresses behind the internal interface is automatically calculated every second (default value) without the need for the administrator to click **Get Interfaces** and install a policy.

To configure dynamic topology updates:

1. Open **Gateway Properties > Network Management**.
2. Select an interface and click **Edit**.
3. In the **Topology** section, click **Modify**.
4. In the **Leads To** section, select **Network defined by routes**.
5. Click **OK**.

This default update value is configured in **SmartConsole > Preferences** and set to one second. The value set here applies to all internal interfaces for all gateways in the domain.

To set the update value for a specific interface:

1. Open **Gateway Properties > Network Management**.
2. Select an interface and click **Actions > Settings**.
3. Select **Use custom update time (seconds)** and set the desired update time.
4. Click **OK**.

Dynamic Anti-Spoofing

When Anti-Spoofing is selected and you click **Get interfaces**, the Security Gateway generates a list of valid IP addresses based on the IP address and netmask of the interface and the routes assigned to the interface.

Anti-Spoofing drops packets with a source IP address that does not belong to the network behind the packet's interface. For example, packets with an internal IP address that comes from an external interface.

When the **Network defined by routes** option is selected along with **Perform Anti-Spoofing based on interface topology**, you get *Dynamic Anti-Spoofing*. The valid IP addresses range is automatically calculated without the administrator having to do click **Get Interfaces** or install a policy.

Secure Internal Communication (SIC)

Check Point platforms and products authenticate each other through one of these Secure Internal Communication (SIC) methods:

- Certificates.
- Standards-based TLS for the creation of secure channels.
- 3DES or AES128 for encryption.

  Gateways above R71 use AES128 for SIC. If one of the gateways is below R71, the gateways use 3DES.

SIC creates trusted connections between gateways, management servers and other Check Point components. Trust is required to install polices on gateways and to send logs between gateways and management servers.

Initializing Trust

To establish the initial trust, a gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.

Note - Make sure the clocks of the gateway and Security Management Server are synchronized, before you initialize trust between them. You can control the Time and Date settings of Check Point gateways and servers with `cpconfig`.

To initialize Trust:

1. In SmartConsole, open the gateway network object.
2. In the **General Properties** page of the gateway, click **Communication**.
3. In the **Communication** window, enter the **Activation Key** that you created during installation of the gateway.
4. Click **Initialize**.

   The ICA signs and issues a certificate to the gateway.

   Trust state is **Initialized but not trusted**. The Internal Certificate Authority (ICA) issues a certificate for the gateway, but does not yet deliver it.

   The two communicating peers authenticate over SSL with the shared Activation Key. The certificate is downloaded securely and stored on the gateway. The Activation Key is deleted.

   The gateway can communicate with Check Point hosts that have a security certificate signed by the same ICA.

SIC Status

After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:

- **Communicating** - The secure communication is established.
- **Unknown** - There is no connection between the gateway and Security Management Server.
- **Not Communicating** - The Security Management Server can contact the gateway, but cannot establish SIC. A message shows more information.

Trust State

If the Trust State is compromised (keys were leaked, certificates were lost) or objects changed (user leaves, open server upgraded to appliance), reset the Trust State. When you reset Trust, the SIC certificate is revoked.

The Certificate Revocation List (CRL) is updated for the serial number of the revoked certificate. The ICA signs the updated CRL and issues it to all gateways during the next SIC connection. If two gateways have different CRLs, they cannot authenticate.

1. In SmartConsole, open the **General Properties** window of the gateway.
2. Click **Communication**.
3. In the **Trusted Communication** window that opens, click **Reset**.
4. **Install Policy** on the gateways.

   This deploys the updated CRL to all gateways. If you do not have a Rule Base (and therefore cannot install a policy), you can reset Trust on the gateways.

   Important - Before a new trust can be established in SmartConsole, make sure the same one-time activation password is configured on the gateway.

Troubleshooting SIC

If SIC fails to Initialize:

1. Make sure there is connectivity between the gateway and Security Management Server.
2. Make sure that the Security Management Server and the gateway use the same SIC activation key (one-time password).
3. If the Security Management Server is behind a gateway, make sure there are rules that allow connections between the Security Management Server and the remote gateway. Make sure Anti-spoofing settings are correct.
4. Make sure the name and the IP address of the Security Management Server are in the `/etc/hosts` file on the gateway.

   If the IP address of the Security Management Server mapped through static NAT by its local gateway, add the public IP address of the Security Management Server to the `/etc/hosts` file on the remote gateway. Make sure the IP address resolves to the server's hostname.
5. Make sure the date and the time settings of the operating systems are correct. If the Security Management Server and remote the gateway reside in different time zones, the remote gateway may have to wait for the certificate to become valid.
6. Remove the security policy on the gateway to let all the traffic through: In the command line interface of the gateway, type: `fw unloadlocal`
7. Try to establish SIC again.

Remote User access to resources and Mobile Access

If you install a certificate on a gateway that has the Mobile Access Software Blade already enabled, you must install the policy again. Otherwise, remote users will not be able to reach network resources.

To establish a new trust state for a gateway:

1. Open the command line interface on the gateway.
2. Enter: **cpconfig**
3. Enter the number for **Secure Internal Communication** and press Enter.
4. Enter **y** to confirm.
5. Enter and confirm the activation key.
6. When done, enter the number for **Exit**.
7. Wait for Check Point processes to stop and automatically restart.

In SmartConsole:

1. In the **General Properties** window of the gateway, click **Communication**.
2. In the **Trusted Communication** window, enter the one-time password (activation key) that you entered on the gateway.
3. Click **Initialize**.
4. Wait for the **Certificate State** field to show **Trust established**.
5. Click **OK**.

Understanding the Check Point Internal Certificate Authority (ICA)

The ICA (Internal Certificate Authority) is created on the Security Management Server when you configure it for the first time. The ICA issues certificates for authentication:

- **Secure Internal Communication (SIC)** - Authenticates communication between Security Management Servers, and between gateways and Security Management Servers.
- **VPN certificates for gateways** - Authentication between members of the VPN community, to create the VPN tunnel.
- **Users** - For strong methods to authenticate user access according to authorization and permissions.

ICA Clients

In most cases, certificates are handled as part of the object configuration. To control the ICA and certificates in a more granular manner, you can use one of these ICA clients:

- The *Check Point configuration utility* - This is the `cpconfig` CLI utility. One of the options creates the ICA, which issues a SIC certificate for the Security Management Server.
- *SmartConsole* - SIC certificates for Security Gateways and administrators, VPN certificates, and user certificates.
- *ICA Management tool* - VPN certificates for users and advanced ICA operations ("The ICA Management Tool" on page 267).

See audit logs of the ICA in SmartConsole **Logs & Monitor** > **New Tab** > **Open Audit Logs View**.

SIC Certificate Management

Manage SIC certificates in the

- **Communication** tab of the gateway properties window.
- ICA Management Tool ("User Certificate Management" on page 269).

Certificates have these configurable attributes:

Attributes	Default	Comments
validity	5 years	
key size	2048 bits	
KeyUsage	5	Digital Signature and Key encipherment
ExtendedKeyUsage	0 (no KeyUsage)	VPN certificates only

To learn more about key size values, see RSA key lengths http://supportcontent.checkpoint.com/solutions?id=sk96591.

Managing Software Blade Licenses

After an administrator runs the First Time Configuration Wizard on a Security Management Server, and the Security Management Server connects to the Internet, it automatically activates its license and synchronizes with the Check Point User Center. If the Security Management Server loses Internet connectivity before the license is activated, it tries again, on an interval.

If the administrator makes changes to Management Software Blade licenses of a Security Management Server in the Check Point User Center, these changes are automatically synchronized with that Security Management Server.

Notes:

- Automatic activation is supported on Check Point appliances only.
- Automatic synchronization is supported on all R80.20.M1 servers.

To make sure that your environment is synchronized with the User Center, even when the Security Management Server is not connected to the Internet, we recommend that you configure a Check Point server with Internet connectivity as a proxy.

In SmartConsole, you can see this information for most Software Blade licenses:

- License status
- Alerts
- Check Point User Center details

See the *R80.20.M1 Release Notes* http://downloads.checkpoint.com/dc/download.htm?ID=65666 for a list of supported Software Blades

Configuring a Proxy gateway

To configure a proxy on a Check Point server:

1. On the Security Management Server, add these lines to `$CPDIR/tmp/.CPprofile.sh`:
   - `_cpprof_add HTTP_CLIENT_PROXY_SICNAME "<proxy server sic name>" 0 0`
   - `_cpprof_add HTTP_CLIENT_PROXY_IP "<proxy server IP>" 0 0`
2. Reboot the Security Management Server.

Viewing Licenses in SmartConsole

To view license information:

In SmartConsole, go to the **Gateways & Servers** view, and from the **Columns** drop-down list, select **Licenses**.

You can see these columns:

Column	Description
License Status	The general state of the Software Blade licenses: • **OK** - All the blade licenses are valid. • **Not Activated** - Blade licenses are not installed. This is only possible in the first 15 days after the establishment of the SIC with the Security Management Server. After the initial 15 days, the absence of licenses will result in the blade error message. • **Error with <number> blade(s)** - The specified number of blade licenses are not installed or not valid. • **Warning with <number> blade(s)** - The specified number of blade licenses have warnings. • **N/A** - No available information.
CK	Unique Certificate Key of the license instance.
SKU	Catalog ID from the Check Point User Center.
Account ID	User's account ID.
Support Level	Check Point level of support.
Support Expiration	Date when the Check Point support contract expires.

To view license information per Software Blade:

1. Select a Security Gateway or a Security Management Server.
2. In the **Summary** tab below, click the object's **License Status** (for example: **OK**).

   The **Device & License Information** window opens. It shows basic object information and **License Status**, license **Expiration Date**, and important quota information (in the **Additional Info** column) for each Software Blade.

Notes:

- Quota information, quota-dependent license statuses, and blade information messages are only supported for R80.
- The tooltip of the SKU is the product name.

The possible values for the Software Blade **License Status** are:

Status	Description
Active	The Software Blade is active and the license is valid.
Available	The Software Blade is not active, but the license is valid.
No License	The Software Blade is active but the license is not valid.
Expired	The Software Blade is active, but the license expired.
About to Expire	The Software Blade is active, but the license will expire in thirty days (default) or less (7 days or less for an evaluation license).
Quota Exceeded	The Software Blade is active, and the license is valid, but the quota of related objects (gateways, files, virtual systems, and so on, depending on the blade) is exceeded.
Quota Warning	The Software Blade is active, and the license is valid, but the number of objects of this blade is 90% (default) or more of the licensed quota.
N/A	The license information is not available.

Monitoring Licenses

To keep track of license issues, you can use these options:

Option	Description
License Status view	To see and export license information for Software Blades on each specific Security Management Server, gateway, or Log Server object.
License Status report	To see, filter and export license status information for all configured Security Management Server, gateway, or Log Server objects.
License Inventory report	To see, filter and export license information for Software Blades on all configured Security Management Server, gateway, or Log Server objects.

The SmartEvent Software Blade lets you customize the **License Status** and **License Inventory** information from the **Logs & Monitor** view of SmartConsole.
It is also possible to view license information from the **Gateways & Servers** view of SmartConsole without enabling the SmartEvent blade on Security Management Server.

The Gateways & Servers view in SmartConsole lets you see and export the *License Inventory* report.

1. **To see the License Inventory report from the Gateways & Servers view:**
   a) In SmartConsole, from the left Navigation Toolbar, click **Gateways & Servers**.
   b) From the top toolbar, click **Actions** > **License Report**.
   c) Wait for the **SmartView** to load and show this report.

      By default, this report contains:

      - *Inventory* page: Blade Names, Devices Names, License Statuses
      - *License by Device* page: Devices Names, License statuses, CK, SKU, Account ID, Support Level, Next Expiration Date
2. **To export the License Inventory report from the Gateways & Servers view:**
   a) In the top right corner, click the **Options** button.
   b) Select the applicable export option - **Export to Excel**, or **Export to PDF**.

The Logs & Monitor view in SmartConsole lets you see, filter and export the *License Status* report.

1. **To see the License Status report from the Logs & Monitor view:**
   a) In SmartConsole, from the left Navigation Toolbar, click **Logs & Monitor**
   b) At the top, open a new tab by clicking **New Tab**, or **[+]**.
   c) In the left section, click **Views**.
   d) In the list of reports, double-click **License Status**.
   e) Wait for the **SmartView** to load and show this report.

      By default, this report contains:

      - Names of the configured objects, License status for each object, CK, SKU, Account ID, Support Level, Next Expiration Date
2. **To filter the License Status report in the Logs & Monitor view:**
   a) In the top right corner, click the **Options** button **> View Filter**.

      The **Edit View Filter** window opens.
   b) Select a **Field** to filter results. For example, **Device Name**, **License Status**, **Account ID**.
   c) Select the logical operator - **Equals**, **Not Equals**, or **Contains**.
   d) Select or enter a filter value.

      Note - Click the **X** icon to delete a filter.
   e) Optional: Click the **+** icon to configure additional filters.
   f) Click **OK** to apply the configured filters.

      The report is filtered based on the configured filters.
3. **To export the License Status report in the Logs & Monitor view:**
   a) In the top right corner, click the **Options** button.
   b) Select the applicable export option - **Export to Excel**, or **Export to PDF**.

The Logs & Monitor view in SmartConsole lets you see, filter and export the *License Inventory* report.

1. **To see the License Inventory report from the Logs & Monitor view:**
   a) In SmartConsole, from the left Navigation Toolbar, click **Logs & Monitor**
   b) At the top, open a new tab by clicking **New Tab**, or **[+]**.
   c) In the left section, click **Reports**.
   d) In the list of reports, double-click **License Inventory**.
   e) Wait for the **SmartView** to load and show this report.

      By default, this report contains:

      - *Inventory* page: Blade Names, Devices Names, License Statuses
      - *License by Device* page: Devices Names, License statuses, CK, SKU, Account ID, Support Level, Next Expiration Date
2. **To filter the License Inventory report in the Logs & Monitor view:**
   a) In the top right corner, click the **Options** button **> Report Filter**.

      The **Edit Report Filter** window opens.
   b) Select a **Field** to filter results. For example, **Blade Name**, **Device Name**, **License Overall Status**, **Account ID**.
   c) Select the logical operator - **Equals**, **Not Equals**, or **Contains**.
   d) Select or enter a filter value.

      Note - Click the **X** icon to delete a filter.
   e) Optional: Click the **+** icon to configure additional filters.
   f) Click **OK** to apply the configured filters.

      The report is filtered based on the configured filters.
3. **To export the License Inventory report in the Logs & Monitor view:**
   a) In the top right corner, click the **Options** button.
   b) Select the applicable export option - **Export to Excel**, or **Export to PDF**.

Managing Objects

In This Section:

Network Objects, defined in SmartConsole and stored in the proprietary Check Point object database, represent physical and virtual network components (such as gateways, servers, and users), and logical components (such as IP address ranges and Dynamic Objects). Before you create Network Objects, analyze the needs of your organization:

- What are the physical components of your network: devices, hosts, gateways and their active Software Blades?
- What are the logical components: services, resources, applications, ranges?
- Who are the users? How should you group them, and with what permissions?

Object Categories

Objects in SmartConsole represent networks, devices, protocols and resources. SmartConsole divides objects into these categories:

Icon	Object Type	Examples
	Network Objects	Gateways, hosts, networks, address ranges, dynamic objects, security zones
	Services	Services, Service groups
	Custom Applications/Sites	Applications, Categories, Mobile applications
	VPN Communities	Site to Site or Remote Access communities
	Users	Users, user groups, and user templates
	Data Types	International Bank Account Number - IBAN, HIPAA - Medical Record Number - MRN, Source Code.
	Servers	Trusted Certificate Authorities, RADIUS, TACACS
	Time Objects	Time, Time groups
	UserCheck Interactions	Message windows: Ask, Cancel, Certificate Template, Inform, and Drop

Icon	Object Type	Examples
	Limit	Download and upload bandwidth

Adding, Editing, Cloning, Deleting, and Replacing Objects

You can add, edit, delete, and clone objects. A clone is a copy of the original object, with a different name. You can also replace one object in the Policy with another object.

Note - Do not create two objects with the same name. You will see a validation error when you try to publish. To resolve, change one of the object names.

To work with objects, right-click the object in the object tree or in the Object Explorer, and select the action.

You can delete objects that are not used, and you can find out where an object is used.

To clone an object:

1. In the object tree or in the Object Explorer, right-click the object and select **Clone**.
   The **Clone Object** window opens.
2. Enter a name for the cloned object.
3. Click **OK**.

To find out where an object is used:

In the object tree or in the Object Explorer, right-click the object and select **Where Used**.

To replace an object with a different object:

1. In the object tree or in the Object Explorer, right-click the object and select **Where Used**.
2. Click the **Replace** icon.
3. From the **Replace with** list, select an item.
4. Click **Replace**.

To delete all instances of an object:

1. In the object tree or in the Object Explorer, right-click the object and select **Where Used**.
2. Click the **Replace** icon.
3. From the **Replace with** list, select **None (remove item)**.
4. Click **Replace**.

Object Tags

Object tags are keywords or labels that you can assign to the network objects or groups of objects for search purposes. These are the types of tags you can assign:

- User tags - Assigned manually to individual objects or groups of objects
- System tags - Predefined keywords, such as "application"

Each tag has a name and a value. The value can be static, or dynamically filled by detection engines.

To add a tag to an object:

1. Open the network object for editing.
2. In the **Add Tag** field, enter the label to associate with this object.
3. Press **Enter**.
   The new tag shows to the right of the **Add Tag** field.
4. Click **OK**.

Network Object Types

In This Section:

Networks

A Network is a group of IP addresses defined by a network address and a net mask. The net mask indicates the size of the network.

A Broadcast IP address is an IP address which is destined for all hosts on the specified network. If this address is included, the Broadcast IP address will be considered as part of the network.

Network Groups

A network group is a collection of hosts, gateways, networks or other groups.

Groups are used where you cannot work with single objects, e.g. when working with VPN domains or with topology definitions.

Groups facilitate and simplify network management. Modifications are applied to the group instead of each member of the group.

To create a group of network objects:

1. In the **Objects** tree, click **New > Network Group**.
   The **New Network Group** window opens.
2. Enter a name for the group
3. Set optional parameters:
   - Object comment
   - Color
   - Tag (as custom search criteria)

4. For each network object or a group of network objects, click the [**+**] sign and select it from the list that shows.
5. Click **OK**.

Check Point Hosts

A Check Point Host can have multiple interfaces but no routing takes place. It is an endpoint that receives traffic for itself through its interfaces. (In comparison, a Security Gateway routes traffic between its multiple interfaces.) For example, if you have two unconnected networks that share a common Security Management Server and Log Server, configure the common server as a Check Point Host object.

A Check Point Host has one or more Software Blades installed. But if the Firewall blade is installed on the Check Point Host, it cannot function as a firewall. The Host requires SIC and other features provided by the actual firewall.

A Check Point Host has no routing mechanism, is not capable of IP forwarding, and cannot be used to implement Anti-spoofing. If the host must do any of these, convert it to be a Security Gateway.

The Security Management Server object is a Check Point Host.

Note - When you upgrade to R80.20.M1 from R77.30 or earlier versions, Node objects are converted to Host objects.

Gateway Cluster

A gateway cluster is a group of Security Gateways with Cluster software installed: ClusterXL, or another Clustering solution. Clustered gateways add redundancy through High Availability or Load Sharing.

Online Services

Online Cloud Service providers always modify IP addresses and Domains that allow access to their services. Administrators who have to maintain up-to-date access control, need an easy way to keep the policy current with the relevant IP addresses and Domains. The Check Point Security Gateways automatically request updates every few hours from online service providers. When updates are available, they are automatically downloaded.

Note - This feature is only supported for R80.20 and above gateways.

Adding an Online Service Object to the Security Policy

This use case shows an Access Control Policy for dynamically updating information from Online Cloud Service providers.

Use Case – Adding an Online Service Object to your Security Policy

A customer has Office365 and wants to make sure that up-to-date IP address and Domain updates are automatically installed on his gateway.

In the example below, add a rule to allow access to Microsoft OneNote. When you add a OneNote object, this ensures that up-to-date IP addresses and Domains from Office365 are added to the Security Policy. Any updates from Office365 that follow are automatically installed because these objects are in the Rule Base.

To add an Online Service object to the Security Gateway:

1. Go to SmartConsole > **Security Policies.**
2. Click the plus sign to add a new rule.
   a) Name the rule.
   b) Click the plus sign from the **Destination** column to access the **Online Services** button.
      The **Online Services** window shows.
   c) Select the objects to add. For this use case, select the **OneNote** object.
      Note - You can also add objects to the **Source** column.
3. Click **OK**.
4. Install policy.

The OneNote object is added to the Rule Base.

No	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Accept OneNote	WirelessZone	OneNote	Any	Any	Accept	Log
2	Accept OneNote	OneNote	WirelessZone	Any	Any	Accept	Log

You can monitor the updates by checking the logs.

To monitor the updates:

1. Go to SmartConsole > **Logs & Monitor.**
2. From the search bar, enter Online Services.
   The **Log Details** window shows.
3. Succeeded shows in the **Status** field when the update is successful.

The Online Cloud Services that are currently supported are Office365 and AWS.

More Network Object Types

Address Ranges

An address range is a range of IP addresses on the network, defined by the lowest and the highest IP addresses. Use an Address Range object when you cannot define a range of IP addresses by a network IP and a net mask. The Address Range objects are also necessary for the implementation of NAT and VPN.

Using Wildcard Objects

Wildcard objects let you define IP address objects that share a common pattern that can be permitted or denied access in a security policy.

Note - This feature is only supported for R80.20 and above gateways.

To create a new wildcard object:

1. Open **Object Explorer** > **New** > **More** > **Network Object** > **Wildcard object**.
2. Enter the Wildcard IP address and Wildcard Netmask in IPv4 or IPv6 Format.
3. Click **OK**.

Understanding Wildcard Objects

The wildcard object contains a wildcard IP address and a wildcard netmask.

The *wildcard netmask* is the mask of bits that indicate which parts of the IP address must match and which do not have to match. For example:

Wildcard IP:	194.	29.	0.	1
Wildcard Netmask:	0.	0.	3.	0

The third octet represents the mask of bits. If we convert the 3 to binary, we get 00000011. The 0 parts of the mask must match the equivalent bits of the IP address. The 1 parts of the mask do not have to match, and can be any value.

0 0 0 0 0 0	1 1
Must match the equivalent bits in the IP address	Do not have to match

The binary netmask produces these possible decimal values:

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**	
						Binary		**Decimal**
0	0	0	0	0	0	0	0	**0**
0	0	0	0	0	0	0	1	**1**
0	0	0	0	0	0	1	0	**2**
0	0	0	0	0	0	1	1	**3**

The netmask permits only these IP addresses:

- 194.29.0.1
- 194.29.1.1
- 192.29.2.1
- 194.29.3.1

Use Cases

Scenario One

A supermarket chain has all of its cash registers on subnet 194.29.x.1, where x defines the region. In this use case, all the cash registers in this region must have access to the database server at 194.30.1.1.

Instead of defining 256 hosts (194.29.0.1, 194.29.1.1, 194.29.2.1....194.29.255.1), the administrator creates a wildcard object that represents all the cash registers in the region:

Wildcard IP:	194.	29.	0.	1

Wildcard Mask:	0.	0.	255.	0

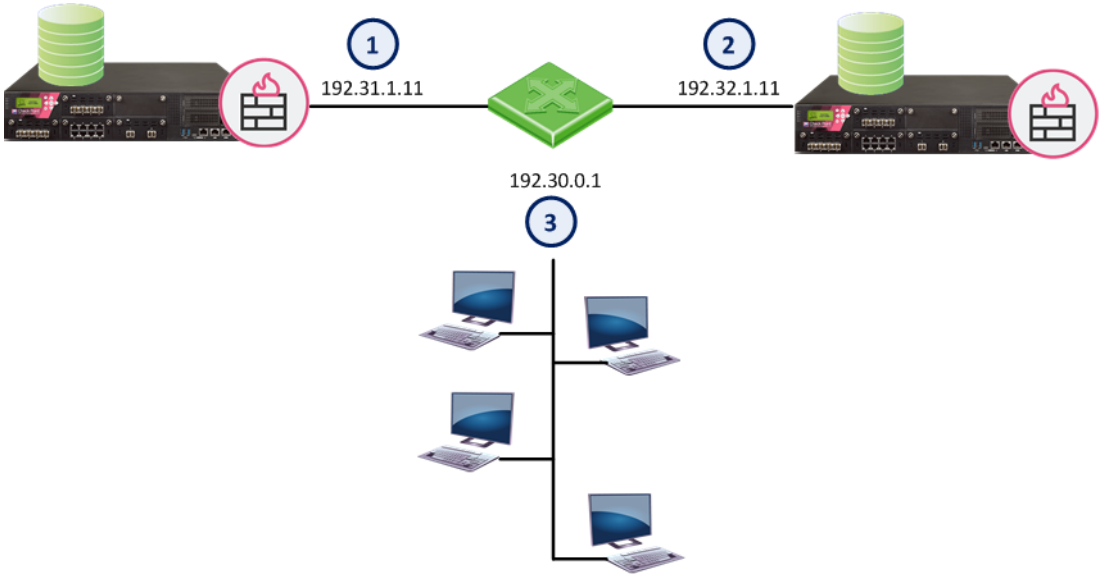
The wildcard object can now be added to the access control policy.

Source	Destination	Action	Track
Wildcard Object	Database server object	Accept	Log

Scenario Two

In this use case, a supermarket chain has stores in Europe and Asia.

The 192.30.0-255.1 network contains both the Asian and European regions, and the stores within those regions.



Item	Description
1	Database Server for Europe
2	Database Server for Asia
3	European and Asia network

The administrator wants stores in the European and Asia regions to access different database servers. In this topology, the third octet of the European and Asia network's IP address will be subject to a wildcard. The first four bits of the wildcard will represent the region and the last four bits will represent the store number.

Bits that represent the region	**Bits that represent the store number**
0000	0000

In the Wildcard IP:

- The Asia region is represented by **0001xxxx** (Region **1** in decimal)
- The European region is represented by **0010xxxx** (Region **2** in decimal)

In binary:

Binary		Decimal
Region	**Store**	
0001	0000	16 - Asia Region
0010	0000	32 - European Region

To include all the stores of a particular region, the last four bits of the wildcard mask must be set to 1 (15 in Decimal):

Binary		Decimal
Region	**Store**	
xxxx	1111	15 - all Asian stores
xxxx	1111	15 - all European stores

A wildcard object that represents all the Asian stores will look like this:

Wildcard IP address	192.30.16.1	(The region)
Wildcard netmask	0.0.15.0	(for stores in the region)

For this range of IP addresses: 192.30.**16-31**.1

A wildcard object that represents all the European stores will look like this:

Wildcard IP address	192.30.32.1	(the region)
Wildcard netmask	0.0.15.0	(for stores in the region)

For this range of IP addresses: 192.30.**32-47**.1

The administrator can now use these wildcard objects in the access control policy:

Source	Destination	Action	Track
Asian Stores Wildcard	Database Server for Asia	Accept	Log
European Stores Wildcard	Database Server for Europe	Accept	Log

Scenario Three

In this scenario, the netmask bits are not consecutive.

Wildcard IP	1	1	0	1
Wildcard mask	0	0	5	0

Wildcard IP	00000001.00000001.00000000.00000001
Wildcard Mask	00000000.00000000.00000101.00000000

Mask:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0

Which will match only these IP addresses:

IP Address	Binary	Comment
1.1.0.1	00000001.00000001.00000000.00000001	The IP address itself
1.1.1.1	00000001.00000001.00000001.00000001	The equivalent bit at position 23 does not matter
1.1.4.1	00000001.00000001.00000100.00000001	The equivalent bit at position 21 does not matter
1.1.5.1	00000001.00000001.00000101.00000001	The equivalent bits at positions 21 and 23 do not matter

IPv6

The same principles apply to IPv6 addresses. For example, if the wildcard object has these values:

IPv6 Address	2001::1:10:0:1:41
Wildcard netmask	0::ff:0:0

The wildcard will match: 2001::1:10:0-255:1:41

Domains

A Domain object lets you define a host or DNS domain by its name only. It is not necessary to have the IP address of the site.

You can use the Domain object in the source and destination columns of an Access Control Policy.

You can configure a Domain object in two ways:

- Select **FQDN**

  In the object name, use the Fully Qualified Domain Name (FQDN). Use the format `.x.y.z` (with a dot "." before the FQDN). For example, if you use `.www.example.com` then the Gateway matches `www.example.com`

  This option is supported for R80.10 and higher, and is the default. It is more accurate and faster than the non-FQDN option.

  The Security Gateway looks up the FQDN with a direct DNS query, and uses the result in the Rule Base.

This option supports SecureXL Accept templates. Using domain objects with this option in a rule has no effect on the performance of the rule, or of the rules that come after it.

- Clear **FQDN**

  This option enforces the domain and its sub-domains. In the object name, use the format `.x.y` for the name. For example, use `.example.com` or `.example.co.uk` for the name. If you use `.example.com`, then the Gateway matches `www.example.com` and `support.example.com`

  The Gateway does the name resolution using DNS reverse lookups, which can be inaccurate. The Gateway uses the result in the Rule Base, and caches the result to use again.

  When upgrading from R77, this option is enforced.

Dynamic Objects

A dynamic object is a "logical" object where the IP address is resolved differently for each Security Gateway, using the `dynamic_objects` command.

For R80.10 Security Gateways and higher, dynamic objects support SecureXL Accept templates. Therefore, there is no performance impact on a rule that uses a dynamic object, or on rules that come after it.

Dynamic Objects are predefined for **LocalMachine-all-interfaces**. The DAIP computer interfaces (static and dynamic) are resolved into this object.

Security Zones

Security Zones let you to create a strong Access Control Policy that controls the traffic between parts of the network.

A Security Zone object represents a part of the network (for example, the internal network or the external network). You assign a network interface of a Security Gateway to a Security Zone. You can then use the Security Zone objects in the Source and Destination columns of the Rule Base.

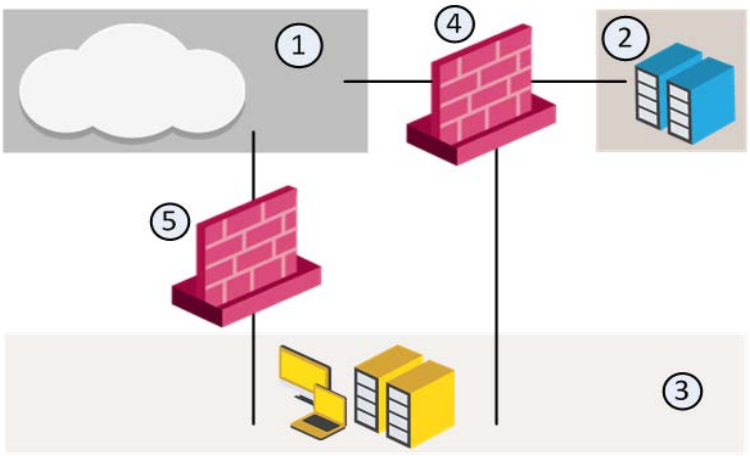
Use Security Zones to:

- Simplify the Policy. Apply the same rule to many Gateways.
- Add networks to Gateways interfaces without changing the Rule Base.

For example, in the diagram, we have three Security Zones for a typical network: *ExternalZone* (1), *DMZZone* (2) and *InternalZone* (3).

- Gateway (4) has three interfaces. One interface is assigned to *ExternalZone* (1), one interface is assigned to *DMZZone* (2), and one interface is assigned to *InternalZone* (3).

- Gateway (5) has two interfaces. One interface is assigned to *ExternalZone* (1) and one interface is assigned to *InternalZone* (3).



A Security Gateway interface can belong to only one Security Zone. Interfaces to different networks can be in the same Security Zone.

Workflow

1. Define Security Zone objects. Or, use the predefined Security Zones (on page 64).
2. Assign Gateway interfaces to Security Zones ("Creating and Assigning Security Zones " on page 63).
3. Use the Security Zone objects in the Source and Destination of a rule. For example:

Source	Destination	VPN	Service	Action
InternalZone	ExternalZone	Any Traffic	Any	Accept

1. Install the Access Control Policy ("Installing the Access Control Policy" on page 110).

Creating and Assigning Security Zones

Before you can use Security Zones in the Rule Base, you must assign Gateway interfaces to Security Zones.

To create a Security Zone:

1. In the **Objects bar** (F11), click **New** > **More** > **Network Object** > **Security Zone**.
   The **Security Zone** window opens.
2. Enter a name for the Security Zone.
3. Enter an optional comment or tag.
4. Click **OK**.

To assign an interface to a Security Zone

1. In the **Gateways & Servers** view, right-click a Security Gateway object and select **Edit**.
   The **Gateway Properties** window opens.
2. In the **Network Management** pane, right-click an interface and select **Edit**.
   The **Interface** window opens. The **Topology** area of the **General** pane shows the Security Zone to which the interface is already bound. By default, the Security Zone is calculated according to where the interface **Leads To**.
3. Click **Modify**.

The **Topology Settings** window opens.

4. In the **Security Zone** area, click **User Defined** and select **Specify Security Zone**.
5. From the drop-down box, select a Security Zone.

   Or click **New** to create a new one.
6. Click **OK**.

Predefined Security Zones

These are the predefined security zones, and their intended purposes:

- **WirelessZone** - Networks that can be accessed by users and applications with a wireless connection.
- **ExternalZone** - Networks that are not secure, such as the Internet and other external networks.
- **DMZZone** - A DMZ (demilitarized zone) is sometimes referred to as a *perimeter* network. It contains company servers that can be accessed from external sources.

  A DMZ lets external users and applications access specific internal servers, but prevents the external users accessing secure company networks. Add rules to the firewall Rule Base that allow traffic to the company DMZ. For example, a rule that allows HTTP and HTTPs traffic to your web server in the DMZ.
- **InternalZone** - Company networks with sensitive data that must be protected and used only by authenticated users.

Externally Managed Gateways/Hosts

An Externally Managed Security Gateway or a Host is a gateway or a Host which has Check Point software installed on it. This Externally Managed gateway is managed by an external Security Management Server. While it does not receive the Check Point Security Policy, it can participate in Check Point VPN communities and solutions.

Interoperable Devices

An Interoperable Device is a device that has no Check Point Software Blades installed. The Interoperable Device:

- Cannot have a policy installed on it
- Can participate in Check Point VPN communities and solutions.

VoIP Domains

There are five types of VoIP Domain objects:

- VoIP Domain SIP Proxy
- VoIP Domain H.323 Gatekeeper
- VoIP Domain H.323 Gateway
- VoIP Domain MGCP Call Agent
- VoIP Domain SCCP CallManager

In many VoIP networks, the control signals follow a different route through the network than the media. This is the case when the call is managed by a *signal routing* device. Signal routing is done

in SIP by the *Redirect Server*, *Registrar*, and/or *Proxy*. In SIP, signal routing is done by the *Gatekeeper* and/or *gateway*.

Enforcing signal routing locations is an important aspect of VoIP security. It is possible to specify the endpoints that the signal routing device is allowed to manage. This set of locations is called a *VoIP Domain*. For more information refer to the *R80.10 VoIP Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54844.

Logical Servers

A Logical Server is a group of machines that provides the same services. The workload of this group is distributed between all its members.

When a Server group is stipulated in the **Servers group** field, the client is bound to this physical server. In Persistent server mode the client and the physical server are bound for the duration of the session.

- Persistency by Service — once a client is connected to a physical server for a specified service, subsequent connection to the same Logical Server and the same service will be redirected to the same physical server for the duration of the session.
- Persistency by Server — once a client is connected to a physical server, subsequent connections to the same Logical Server (for any service) will be redirected to the same physical server for the duration of the session.

Balance Method

The load balancing algorithm stipulates how the traffic is balanced between the servers. There are several types of balancing methods:

- **Server Load** — The Security Gateway determines which Security Management Server is best equipped to handle the new connection.
- **Round Trip Time** — On the basis of the shortest round trip time between Security Gateway and the servers, executed by a simple ping, the Security Gateway determines which Security Management Server is best equipped to handle the new connection.
- **Round Robin** — the new connection is assigned to the first available server.
- **Random** — the new connection is assigned to a server at random.
- **Domain** — the new connection is assigned to a server based on domain names.

Open Security Extension (OSE) Devices

The Open Security Extension features let you manage third-party devices with the Check Point SmartConsole. The number of managed devices, both hardware and software packets, depends on your license. OSE devices commonly include hardware security devices for routing or dedicated Network Address Translation and Authentication appliances. Security devices are managed in the Security Policy as Embedded Devices.

The Security Management Server generates Access Lists from the Security Policy and downloads them to selected routers and open security device. Check Point supports these devices:

OSE Device	Supported Versions
Cisco Systems	9.x, 10.x, 11.x, 12.x

The Check Point Rule Base must not have these objects. If it does, the Security Management Server will not generate Access Lists.

- Drop (in the Action column)
- Encrypt (Action)
- Alert (Action)
- RPC (Service)
- ACE (Service)
- Authentication Rules
- Negate Cell

Defining OSE Device Interfaces

OSE devices report their network interfaces and setup at boot time. Each OSE device has a different command to list its configuration. You must define at least one interface for each device, or Install Policy will fail.

To define an OSE Device:

1. From the Object Explorer, click **New** > **More**.
2. Click Network **Object** > **More** > **OSE Device**.
3. Enter the general properties ("OSE Device Properties Window — General Tab" on page 66).
   We recommend that you also add the OSE device to the host lists on other servers: `hosts` (Linus) and `lmhosts` (Windows).
4. Open the **Topology** tab and add the interfaces of the device.
   You can enable Anti-Spoofing on the external interfaces of the device. Double-click the interface. In the **Interface Properties** window > **Topology** tab, select **External** and **Perform Anti-Spoofing**.
5. Open the **Setup** tab and define the OSE device and its administrator credentials (see "Anti-Spoofing Parameters and OSE Devices Setup (Cisco)" on page 66).

OSE Device Properties Window — General Tab

- **Name** — The name of the OSE device, as it appears in the system database on the server.
- **IP Address** — The device's IP address.
- **Get Address** — Click this button to resolve the name to an address.
- **Comment** — Text to show on the bottom of the **Network Object** window when this object is selected.
- **Color** — Select a color from the drop-down list. The OSE device will be represented in the selected color in SmartConsole, for easier tracking and management.
- **Type** — Select from the list of supported vendors.

Anti-Spoofing Parameters and OSE Devices Setup (Cisco)

For Cisco (Version 10.x and higher) devices, you must specify the direction of the filter rules generated from anti-spoofing parameters. The direction of enforcement is specified in the **Setup** tab of each router.

For Cisco routers, the direction of enforcement is defined by the **Spoof Rules Interface Direction** property.

Access List No — The number of Cisco access lists enforced. Cisco routers Version 12x and below support an ACL number range from 101-200. Cisco routers Version 12x and above support an ACL

range number from 101-200 and also an ACL number range from 2000-2699. Inputting this ACL number range enables the support of more interfaces.

For each credential, select an option:

- **None** — Credential is not needed.
- **Known** — The administrator must enter the credentials.
- **Prompt** — The administrator will be prompted for the credentials.

Username — The name required to logon to the OSE device.

Password — The Administrator password (Read only) as defined on the router.

Enable Username — The user name required to install Access Lists.

Enable Password — The password required to install Access Lists.

Version — The Cisco OSE device version (9.x, 10.x, 11.x, 12.x).

OSE Device Interface Direction — Installed rules are enforced on data packets traveling in this direction on all interfaces.

Spoof Rules Interface Direction — The spoof tracking rules are enforced on data packets traveling in this direction on all interfaces.

Managing Policies

In This Section:

SmartConsole offers a number of tools that address policy management tasks, both at the definition stage and for maintenance.

At the definition stage:

- *Policy Packages* let you group different types of policies, to be installed together on the same installation targets.
- *Predefined Installation Targets* let you associate each package with a set of gateways. You do not have to repeat the gateway selection process each time you install a Policy Package.

At the maintenance level:

- *Search* gives versatile search capabilities for network objects and the rules in the Rule Base.
- *Database version control* lets you track past changes to the database.

Working with Policy Packages

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

- **Access Control** - consists of these types of rules**:**
  - Firewall
  - NAT
  - Application & URL Filtering
  - Content Awareness
- **QoS** - Quality of Service rules for bandwidth management
- **Desktop Security** - the Firewall policy for endpoint computers that have the Endpoint Security VPN remote access client installed as a standalone client.
- **Threat Prevention** - consists of:
  - IPS - IPS protections continually updated by IPS Services
  - Anti-Bot - Detects bot-infected machines, prevents bot damage by blocking bot commands and Control (C&C) communications
  - Anti-Virus - Includes heuristic analysis, stops viruses, worms, and other malware at the gateway
  - Threat Emulation - Detects zero-day and advanced polymorphic attacks by opening suspicious files in a sandbox
  - Threat Extraction - Extracts potentially malicious content from e-mail attachments before they enter the corporate network

The installation process:

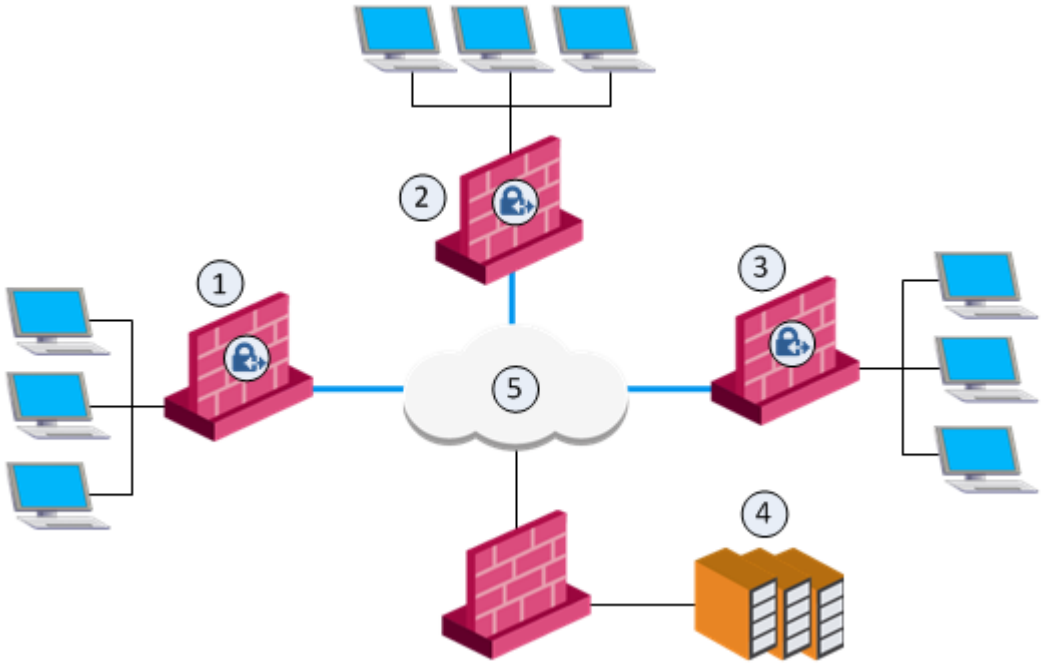
- Runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.

  If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.
- Makes sure that each of the Security Gateways enforces at least one of the rules. If none of the rules are enforced, the default drop rule is enforced.
- Distributes the user database and object database to the selected installation targets.

You can create different policy packages for different types of sites in an organization.

Example:

An organization has four sites, each with its own requirements. Each site has a different set of Software Blades installed on the Security Gateways:



Item	Security Gateway	Installed Software Blades
1	Sales California	Firewall, VPN
2	Sales Alaska	Firewall, VPN, IPS, DLP
3	Executive management	Firewall, VPN, QoS, and Mobile Access
4	Server farm	Firewall
5	Internet	

To manage these different types of sites efficiently, you need to create three different Policy Packages. Each Package includes a combination of policy types that correspond to the Software Blades installed on the site's gateway. For example:

- A policy package that includes the Access Control policy type. The Access Control policy type controls the firewall, NAT, Application & URL Filtering, and Content Awareness Software Blades. This package also determines the VPN configuration.

  Install the Access Control policy package on *all* Security Gateways.
- A policy package that includes the QoS policy type for the QoS blade on gateway that manages bandwidth.

  Install this policy package on the *executive management* Gateway.
- A policy package that includes the Desktop Security Policy type for the gateway that handles Mobile Access.

  Install this policy package on the *executive management* Gateway.

Creating a New Policy Package

1. From the Menu, select **Manage Policies**.

   The **Manage Policies** window opens.
2. Click **New**.

   The **Policy** window opens.
3. Enter a name for the policy package.
4. In the **General** page > **Policy types** section, select one or more of these policy types:
   - **Access Control**
   - **Threat Prevention**
   - **QoS**, select **Recommended** or **Express**
   - **Desktop Security**

   You see the **QoS**, and **Desktop Security** policy types only if they are enabled on one or more Gateways.
5. On the **Installation targets** page, select the gateways the policy will be installed on:
   - **All gateways**
   - **Specific gateways** - For each gateway, click the [**+**] sign and select it from the list.

   To install Policy Packages correctly and eliminate errors, each Policy Package is associated with a set of appropriate installation targets.
6. Click **OK**.
7. Click **Close**.

   The new policy shows on the **Security Policies** page.

Adding a Policy Type to an Existing Policy Package

1. From the Menu, select **Manage Policies**.

   The **Manage Policies** window opens.
2. Select a policy package and click the **Edit** button.
3. The **Policy** package window opens.
4. On the **General** > **Policy types** page, select the policy type to add:
   - **Access Control**

- **QoS**, select **Recommended** or **Express**
- **Desktop Security**
- **Threat Prevention**

5. Click **OK**.

Installing a Policy Package

1. On the Global Toolbar, click **Install Policy**.

   The **Install Policy** window opens showing the installation targets (Security Gateways).
2. From the **Select a policy** menu, select a policy package.
3. Select one or more policy types that are available in the package.
4. Select the **Install Mode**:
   - **Install on each selected gateway independently** - Install the policy on each target gateway independently of others, so that if the installation fails on one of them, it doesn't affect the installation on the rest of the target gateways.

     Note - If you select **For Gateway Clusters install on all the members, if fails do not install at all**, the Security Management Server makes sure that it can install the policy on all cluster members before it begins the installation. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all the target gateways. If the policy fails to install on one of the gateways, the policy is not installed on other target gateways.
5. Click **Install**.

Installing the User Database

When you make changes to user definitions through SmartConsole , they are saved to the user database on the Security Management Server. User authentication methods and encryption keys are also saved in this database. The user database does *not* contain information about users defined externally to the Security Gateway (such as users in external User Directory groups), but it does contain information about the external groups themselves (for example, on which Account Unit the external group is defined). Changes to external groups take effect only after the policy is installed, or the user database is downloaded from the Security Management Server.

You must choose to install the policy or the user database, based on the changes you made:

- Install the policy ("Installing a Policy Package" on page 71), if you modified additional components of the Policy Package (for example, added new Security Policy rules) that are used by the installation targets
- Install the user database, if you only changed the user definitions or the administrator definitions - From the Menu, select **Install Database**

The user database is installed on:

- Security Gateways - during policy installation
- Check Point hosts with one or more Management Software Blades enabled - during database installation

You can also install the user database on Security Gateways and on a remote server, such as a Log Server, from the command line interface on the Security Management Server.

To install user database from the command line interface:

On the Security Management Server, run: `fwm dbload <host name>`

Note - Check Point hosts that do not have active Management Software Blades do not get the user database installed on them.

Uninstalling a Policy Package

You can uninstall a policy package through a command line interface on the gateway.

To uninstall a policy package:

1. Open a command prompt on the Security Gateway.
2. Run: `fw unloadlocal`.

Viewing Rule Logs

You can search for the logs that are generated by a specified rule, from the Security Policy or from the Logs & Monitor > **Logs** tab

To see logs generated by a rule (from the Security Policy):

1. In SmartConsole, go to the **Security Policies** view.
2. In the **Access Control Policy** or **Threat Prevention Policy**, select a rule.
3. In the bottom pane, click one of these tabs to see:
   - **Summary** - Rule name, rule action, rule creation information, and the hit count. Add custom information about the rule.
   - **Details** (Access Control Policy only) - Details for each column. Select columns as necessary.
   - **Logs** - By default, shows the logs for the *Current Rule*. You can filter them by **Source**, **Destination**, **Blade**, **Action**, **Service**, **Port**, **Source Port**, **Rule** (**Current rule** is the default), **Origin**, **User**, or **Other Fields**.
   - **History** (Access Control Policy only) - List of rule operations in chronological order, with the information about the rule type and the administrator that made the change.

To see logs generated by a rule (by Searching the Logs):

1. In SmartConsole, go to the **Security Policies** view.
2. In the **Access Control Policy** or **Threat Prevention Policy**, select a rule.
3. Right-click the rule number and select **Copy Rule UID**.
4. In the Logs & Monitor > **Logs** tab, search for the logs in one of these ways:
   - Paste the Rule UID into the query search bar and press Enter.
   - For faster results, use this syntax in the query search bar:

     `layer_uuid_rule_uuid:*_<UID>`

     For example, paste this into the query search bar and press Enter:

     `layer_uuid_rule_uuid:*_46f0ee3b-026d-45b0-b7f0-5d71f6d8eb10`

Policy Installation History

In the Installation History you can choose a Gateway, a date and time when the Policy was installed, and:

- See the revisions that were installed on the Gateway and who installed the Policy.
- See the changes that were installed and who made the changes.
- Revert to a specific version, and install the last "good" Policy.

To work with the Policy installation history:

1. In SmartConsole, go to **Security Policies**.
2. From the **Access Tools** or the **Threat Prevention Tools**, select **Installation History**.
3. In the **Gateways** section, select a Gateway.
4. In the **Policy Installation History** section, select an installation date.
5. **To see the revisions that were installed and who made them**:

   Click **View installed changes**.

   To see the changes that were installed and who made them :

   Click **View**.

   To revert to a specific version of the Policy:

   Click **Install specific version**.

Creating an Access Control Policy

In This Section:

Introducing the Unified Access Control Policy

Define one, unified Access Control Policy. The Access Control Policy lets you create a simple and granular Rule Base that combines all these Access Control features:

- Firewall - Control access to and from the internal network.
- Application & URL Filtering - Block applications and sites.
- Content Awareness - Restrict the Data Types that users can upload or download.
- IPsec VPN and Mobile Access - Configure secure communication with Site-to-Site and Remote Access VPNs.
- Identity Awareness - Identify users, computers, and networks.

There is no need to manage separate Rule Bases. For example, you can define one, intuitive rule that: Allows users in specified networks, to use a specified application, but prevents downloading files larger than a specified size. You can use all these objects in one rule:

- Security Zones
- Services
- Applications and URLs
- Data Types
- Access Roles

Information about these features is collected in one log:

- Network

- Protocol
- Application
- User
- Accessed resources
- Data Types

Creating a Basic Access Control Policy

A firewall controls access to computers, clients, servers, and applications using a set of rules that make up an Access Control Rule Base. You need to configure a Rule Base with secure Access Control and optimized network performance.

A strong Access Control Rule Base:

- Allows only authorized connections and prevents vulnerabilities in a network.
- Gives authorized users access to the correct internal resources.
- Efficiently inspects connections.

Basic Rules

Best Practice - These are basic Access Control rules we recommend for all Rule Bases:

- **Stealth rule** that prevents direct access to the Security Gateway
- **Cleanup rule** that drops all traffic that is not allowed by the earlier rules in the policy

Note - There is also the **implicit drop rule** that drops all traffic that did not match all other rules. This rule does not create log entries. If you want to log the traffic, create an **explicit Cleanup rule**.

Use Case - Basic Access Control

This use case shows a Rule Base for a simple Access Control security policy. (The **Hits**, **VPN** and **Content** columns are not shown.)

No	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Admin Access to Gateways	Admins (Access Role)	Gateways-group	Any	Accept	Log	Policy Targets
2	Stealth	Any	Gateways-group	Any	Drop	Alert	Policy Targets
3	Critical subnet	Internal	Finance HR R&D	Any	Accept	Log	CorpGW
4	Tech support	TechSupport	Remote1-web	HTTP	Accept	Alert	Remote1GW
5	DNS server	Any	DNS	Domain UDP	Accept	None	Policy Targets
6	Mail and Web servers	Any	DMZ	HTTP HTTPS SMTP	Accept	Log	Policy Targets
7	SMTP	Mail	NOT Internal net group	SMTP	Accept	Log	Policy Targets
8	DMZ & Internet	IntGroup	Any	Any	Accept	Log	Policy Targets

No	Name	Source	Destination	Services & Applications	Action	Track	Install On
9	Cleanup rule	Any	Any	Any	Drop	Log	Policy Targets

Rule	Explanation
1	**Admin Access to Gateways** - SmartConsole administrators are allowed to connect to the Security Gateways.
2	**Stealth** - All internal traffic that is NOT from the SmartConsole administrators to one of the Security Gateways is dropped. When a connection matches the Stealth rule, an alert window opens in SmartView Monitor.
3	**Critical subnet** - Traffic from the internal network to the specified resources is logged. This rule defines three subnets as critical resources: Finance, HR, and R&D.
4	**Tech support** - Allows the Technical Support server to access the Remote-1 web server which is behind the Remote-1 Security Gateway. Only HTTP traffic is allowed. When a packet matches the Tech support rule, the Alert action is done.
5	**DNS server** - Allows UDP traffic to the external DNS server. This traffic is not logged.
6	**Mail and Web servers** - Allows incoming traffic to the mail and web servers that are located in the DMZ. HTTP, HTTPS, and SMTP traffic is allowed.
7	**SMTP** - Allows outgoing SMTP connections to the mail server. Does not allow SMTP connections to the internal network, to protect against a compromised mail server.
8	**DMZ and Internet** - Allows traffic from the internal network to the DMZ and Internet.
9	**Cleanup rule** - Drops all traffic that does not match one of the earlier rules.

Use Case - Inline Layer for Each Department

This use case shows a basic Access Control Policy with a sub-policy for each department. The rules for each department are in an Inline Layer. An Inline Layer is independent of the rest of the Rule Base. You can delegate ownership of different Layers to different administrators.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
1	Critical subnet	Internal	Finance HR	Any	Any	Accept	Log
2	SMTP	Mail	NOT internal network (Group)	SMTP	Any	Accept	Log
3	R&D department	R&D Roles	Any	Any	Any	TechSupport Layer	N/A
3.1	R&D servers	Any	R&D servers (Group) QA network	Any	Any	Accept	Log
3.2	R&D source control	InternalZone	Source control servers (Group)	ssh, http, https	Any	Accept	Log
---	---	---	---	---	---	---	---

3.X	Cleanup rule	Any	Any	Any	Any	Drop	Log
4	QA department	QA network	Any	Any	Any	QA Layer	N/A
4.1	Allow access to R&D servers	Any	R&D Servers (Group)	Web Services	Any	Accept	Log
----	---	---	---	---	---	---	---
4.Y	Cleanup rule	Any	Any	Any	Any	Drop	Log
5	Allow all users to access employee portal	Any	Employee portal	Web Services	Any	Accept	None
---	---	---	---	---	---	---	---
9	Cleanup rule	Any	Any	Any	Any	Drop	Log

Rules	Explanation
1 2	General rules for the whole organization.
3 3.1 3.2 --- 3.X	An Inline Layer for the R&D department. Rule 3 is the parent rules of the Inline Layer. The **Action** is the name of the Inline Layer. **If a packet does not match on parent rule 3:** Matching continues to the next rule outside the Inline Layer (rule 4). **If a packet matches on parent rule 3:** Matching continues to 3.1, first rule inside the Inline Layer. If a packet matches on this rule, the rule action is done on the packet. If a packet does not match on rule 3.1, continue to the next rule inside the Inline Layer, rule 3.2. If there is no match, continue to the remaining rules in the Inline Layer. --- means one or more rules. The packet is matched only inside the inline layer. It never leaves the inline layer, because the inline layer has an implicit cleanup rule. It is not matched on rules 4, 5 and the other rules in the Ordered Layer. Rule 3.X is a **cleanup rule**. It drop all traffic that does not match one of the earlier rules in the Inline Layer. This is a default explicit rule. You can change or delete it. **Best Practice -** Have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer.
4 4.1 --- 4.Y	Another Inline Layer, for the QA department.
5	More general rules for the whole organization.
--	One or more rules.

Rules	Explanation
9	**Cleanup rule** - Drop all traffic that does not match one of the earlier rules in the Ordered Layer. This is a default explicit rule. You can change or delete it. **Best Practice -** Have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer.

Creating Application Control and URL Filtering Rules

Create and manage the Policy for Application Control and URL Filtering in the Access Control Policy, in the **Access Control** view of SmartConsole. Application Control and URL Filtering rules define which users can use specified applications and sites from within your organization and what application and site usage is recorded in the logs.

To learn which applications and categories have a high risk, look through the **Application Wiki** in the **Access Tools** part of the **Security Policies** view. Find ideas for applications and categories to include in your Policy.

To see an overview of your Access Control Policy and traffic, see the **Access Control** view in **Logs & Monitor** > **New Tab** > **Views**.

Monitoring Applications

Scenario: I want to monitor all Facebook traffic in my organization. How can I do this?

To monitor all Facebook application traffic:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.
3. Click one of the **Add rule** toolbar buttons to add the rule in the position that you choose in the Rule Base. The first rule matched is applied.
4. Create a rule that includes these components:
   - **Name** - Give the rule a name, such as **Monitor Facebook**.
   - **Source** - Keep it as **Any** so that it applies to all traffic from the organization.
   - **Destination** - Keep it as **Internet** so that it applies to all traffic going to the internet or DMZ.
   - **Services & Applications** - Click the plus sign to open the Application viewer. Add the **Facebook** application to the rule:
     - Start to type "face" in the Search field. In the Available list, see the **Facebook** application.
     - Click each item to see more details in the description pane.
     - Select the items to add to the rule.

     Note - Applications are matched by default on their **Recommended** services. You can change this. ("Configuring Matching for an Allowed Application" on page 95) Each service runs on a specific port. The recommended **Web Browsing Services** are `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`.
   - **Action** - Select **Accept**
   - **Track** - Select **Log**
   - **Install On** - Keep it as **Policy Targets** for or all gateways, or choose specific Security Gateways on which to install the rule

The rule allows all Facebook traffic but logs it. You can see the logs in the **Logs & Monitor** view, in the **Logs** tab. To monitor how people use Facebook in your organization, see the **Access Control** view (SmartEvent Server required).

Blocking Applications and Informing Users

Scenario: I want to block pornographic sites in my organization, and tell the user about the violation. How can I do this?

To block an application or category of applications and tell the user about the policy violation:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.
3. Create a rule that includes these components:
   - **Services & Applications** - Select the **Pornography** category.
   - **Action** - **Drop**, and a UserCheck **Blocked Message - Access Control**

     The message informs users that their actions are against company policy and can include a link to report if the website is included in an incorrect category.
   - **Track** - **Log**

Note - This Rule Base example contains only those columns that are applicable to this subject.

Name	Source	Destination	Services & Applications	Action	Track	Install On
Block Porn	Any	Internet	Pornography (category)	Drop Blocked Message	Log	Policy Targets

The rule blocks traffic to pornographic sites and logs attempts to access those sites. Users who violate the rule receive a UserCheck message that informs them that the application is blocked according to company security policy. The message can include a link to report if the website is included in an incorrect category.

Important - A rule that blocks traffic, with the **Source** and **Destination** parameters defined as **Any**, also blocks traffic to and from the Captive Portal.

Limiting Application Traffic

Scenario: I want to limit my employees' access to streaming media so that it does not impede business tasks.

If you do not want to block an application or category, there are different ways to set limits for employee access:

- Add a **Limit** object to a rule to limit the bandwidth that is permitted for the rule.
- Add one or more **Time** objects to a rule to make it active only during specified times.

The example rule below:

- Allows access to streaming media during non-peak business hours only.
- Limits the upload throughput for streaming media in the company to 1 Gbps.

To create a rule that allows streaming media with time and bandwidth limits:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Choose a Layer with **Applications and URL Filtering** enabled.
3. Click one of the **Add Rule** toolbar buttons to add the rule in the position that you choose in the Rule Base.
4. Create a rule that includes these components:
   - **Services & Applications** - **Media Streams** category.

     Note - Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Services & Applications Column (on page 94).
   - **Action -** Click **More** and select **Action**:*Accept*, and a **Limit** object.
   - **Time** - Add a **Time** object that specifies the hours or time period in which the rule is active.

     Note - The **Time** column is not shown by default in the Rule Base table. To see it, right-click on the table header and select **Time**.

Name	Source	Destination	Services and Applications	Action	Track	Install On	Time
Limit Streaming Media	Any	Internet	Media Streams (Category)	Accept Upload_1Gbps	Log	All	Off-Work

Note - In a cluster environment, the specified bandwidth limit is divided between all defined cluster members, whether active or not. For example, if a rule sets 1Gbps limit in a three member cluster, each member has a fixed limit of 333 Mbps.

Using Identity Awareness Features in Rules

Scenario: I want to allow a Remote Access application for a specified group of users and block the same application for other users. I also want to block other Remote Access applications for everyone. How can I do this?

If you enable Identity Awareness on a Security Gateway, you can use it together with Application Control to make rules that apply to an a*ccess role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role **Identified_Users** that represents all identified users in the organization. You can use this to allow access to applications only for users who are identified on the Security Gateway.
- You want to allow access to the Radmin Remote Access tool for all identified users.
- You want to block all other Remote Access tools for everyone within your organization. You also want to block any other application that can establish remote connections or remote control.

To do this, add two new rules to the Rule Base:

1. Create a rule and include these components:
   - **Source** - The **Identified_Users** access role
   - **Destination** - **Internet**
   - **Services & Applications - Radmin**
   - **Action** - **Accept**
2. Create another rule below and include these components:
   - **Source** - **Any**
   - **Destination** - **Internet**
   - **Services & Applications** - The category: **Remote Administration**
   - **Action** - **Block**

Name	Source	Destination	Services & Applications	Action	Track	Install On
Allow Radmin to Identified Users	Identified_Users	Internet	Radmin	Allow	Log	All
Block other Remote Admins	Any	Internet	Remote Administration	Block	Log	All

Notes on these rules:

- Because the rule that allows Radmin is above the rule that blocks other Remote Administration tools, it is matched first.
- The Source of the first rule is the **Identified_Users** access role. If you use an access role that represents the Technical Support department, then only users from the technical support department are allowed to use Radmin.
- Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web browsing services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories.

For more about Access Roles and Identity Awareness, see the *R80.10 Identity Awareness Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54825.

Blocking Sites

Scenario: I want to block sites that are associated with categories that can cause liability issues. Most of these categories exist in the Application Database but there is also a custom defined site that must be included. How can I do this?

You can do this by creating a *custom group* and adding all applicable categories and the site to it. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an a*ccess role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created
  - An Access Role that represents all identified users in the organization (*Identified_Users*).
  - A custom application for a site named *FreeMovies*.

- You want to block sites that can cause liability issues for everyone within your organization.
- You will create a custom group that includes Application Database categories as well as the previously defined custom site named *FreeMovies*.

To create a custom group:

1. In the Object Explorer, click **New > More > Custom Application/Site > Application/Site Group**.
2. Give the group a name. For example, *Liability_Sites*.
3. Click **+** to add the group members:
   - Search for and add the custom application *FreeMovies*.
   - Select **Categories**, and add the ones you want to block (for example *Anonymizer*, *Critical Risk*, and *Gambling*)
   - Click **Close**
4. Click **OK**.

You can now use the *Liability_Sites* group in the Access Control Rule Base.

In the Rule Base, add a rule similar to this:

In the Security Policies view of SmartConsole, go to the **Access Control** Policy.

- **Source** - The **Identified_Users** access role
- **Destination** - **Internet**
- **Services & Applications** - *Liability_Sites*
- **Action** - **Drop**

  Note - Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web Browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories.

Name	Source	Destination	Services & Applications	Action	Track
Block sites that may cause a liability	Identified_Users	Internet	Liability_Sites	Drop	Log

Blocking URL Categories

Scenario: I want to block pornographic sites. How can I do this?

You can do this by creating a rule that blocks all sites with pornographic material with the *Pornography category*. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an a*ccess role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role (*Identified_Users*) that represents all identified users in the organization.
- You want to block sites related to pornography.

The procedure is similar to *Blocking Applications and Informing Users.*

In the Rule Base, add a rule similar to this:

- **Source** - The *Identified_Users* access role
- **Destination** - **Internet**
- **Services & Applications** - **Pornography** category
- **Action** - Drop

  Note - Categories are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control **Web Browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories.

Ordered Layers and Inline Layers

A policy is a set of rules that the gateway enforces on incoming and outgoing traffic. There are different policies for Access Control and for Threat Prevention.

You can organize the Access Control rules in more manageable subsets of rules using Ordered Layers and Inline Layers.

In This Section

The Need for Ordered Layers and Inline Layers

Ordered Layers and Inline Layers helps you manage your cyber security more efficiently. You can:

- Simplify the Rule Base, or organize parts of it for specific purposes.
- Organize the Policy into a hierarchy, using Inline Layers, rather than having a flat Rule Base.

  An Inline Layer is a *sub-policy* which is independent of the rest of the Rule Base.
- Reuse Ordered Layers in multiple Policy packages, and reuse Inline Layers in multiple Layers.
- Simplify the management of the Policy by delegating ownership of different Layers to different administrators.
- Improve performance by reducing the number of rules in a Layer.

Order of Rule Enforcement in Inline Layers

The Ordered Layer can contain Inline Layers.

This is an example of an Inline Layer:

No.		Source	Destination	VPN	Services	Action
1						
2		Lab_network	Any	Any	Any	Lab_rules
	2.1	Any	Any	Any	https http	Allow
	2.2	Any	Any	Any	Any	Drop
3						

The Inline Layer has a parent rule (Rule 2 in the example), and sub rules (Rules 2.1 and 2.2). The Action of the parent rule is the name of the Inline Layer.

If the packet does not match the parent rule of the Inline Layer, the matching continues to the next rule of the Ordered Layer (Rule 3).

If a packet matches the parent rule of the Inline Layer (Rule 2), the Firewall checks it against the sub rules:

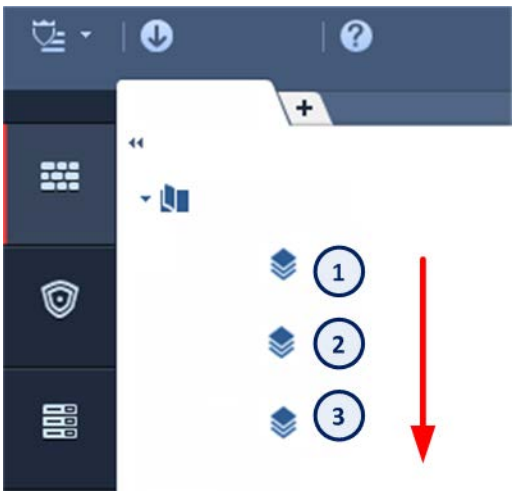
- If the packet matches a sub rule in the Inline Layer (Rule 2.1), no more rule matching is done.
- If none of the higher rules in the Ordered Layer match the packet, the explicit **Cleanup Rule** is applied (Rule 2.2). If this rule is missing, the **Implicit Cleanup Rule** ("Types of Rules in the Rule Base" on page 88) is applied. No more rule matching is done.

Important - Always add an explicit **Cleanup Rule** at the end of each Inline Layer, and make sure that its **Action** is the same as the **Action** of the **Implicit Cleanup Rule**.

Order of Rule Enforcement in Ordered Layers

When a packet arrives at the gateway, the gateway checks it against the rules in the first Ordered Layer, sequentially from top to bottom, and enforces the first rule that matches a packet.

If the **Action** of the matching rule is **Drop**, the gateway stops matching against later rules in the Policy Rule Base and drops the packet. If the **Action** is **Accept**, the gateway continues to check rules in the next Ordered Layer.



Item	Description
1	Ordered Layer 1
2	Ordered Layer 2
3	Ordered Layer 3

If none of the rules in the Ordered Layer match the packet, the explicit **Default Cleanup Rule** is applied. If this rule is missing, the **Implicit Cleanup Rule** ("Types of Rules in the Rule Base" on page 88) is applied.

Every Ordered Layer has its own implicit cleanup rule. You can configure the rule to *Accept* or *Drop* in the Layer settings ("Configuring the Implicit Cleanup Rule" on page 90).

Important - Always add an explicit **Cleanup Rule** at the end of each Ordered Layer, and make sure that its **Action** is the same as the **Action** of the **Implicit Cleanup Rule**.

Creating an Inline Layer

An Inline Layer is a *sub-policy* which is independent of the rest of the Rule Base.

The workflow for making an Inline Layer is:

1. Create a *parent* rule for the Inline Layer. Make a rule that has one or more properties that are the same for all the rules in the Inline Layer. For example, rules that have the same source, or service, or group of users.
2. Create *sub-rules* for the Inline Layer. These are rules that define in more detail what to do if the Firewall matches a connection to the parent rule. For example, each sub-rule can apply to specified hosts, or users, or services, or Data Types.

To create an Inline Layer:

1. Add a rule to the Ordered Layer. This is the *parent* rule.
2. In the **Source**, **Destination**, **VPN**, and **Services & Applications** cells, define the match conditions for the Inline Layer.
3. Click the **Action** cell of the rule. Instead of selecting a standard action, select **Inline Layer** > **New Layer**.
4. The **Layer Editor** window opens.
5. Configure the properties of the Inline Layer:
   a) Enable one or more of these **Blades** for the rules of Inline Layer:
      - **Firewall**
      - **Application & URL Filtering**
      - **Content Awareness**
      - **Mobile Access**
   b) **Optional**: It is a best practice to share Layers with other Policy packages when possible. To enable this select **Multiple policies can use this layer.**
   c) Click **Advanced**.
   d) Configure the **Implicit Cleanup Rule** to *Drop* or *Accept* ("Types of Rules in the Rule Base" on page 88).
   e) Click **OK**.

The name of the Inline Layer shows in the **Action** cell of the rule.

6. Under the parent rule of the Inline Layer, add *sub-rules*.
7. Make sure there is an explicit cleanup rule as the last rule of the Inline Layer ("Types of Rules in the Rule Base" on page 88).

Creating a Ordered Layer

To create a Ordered Layer:

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.
2. In the left pane, click **Layers**.

   You will see a list of the Layers. You can select **Show only shared Layers**.
3. Click the **New** icon in the upper toolbar.
4. Configure the settings in the **Layer Editor** window.
5. **Optional**: It is a best practice to share Layers with other Policy packages when possible. To enable this select **Multiple policies can use this layer.**
6. Click **OK**.
7. Click **Close**.
8. **Publish** the session.

   This Ordered Layer is not yet assigned to a Policy Package.

To add a Ordered Layer to the Access Control Policy:

1. In SmartConsole, click **Security Policies**.
2. Right-click a Layer in the **Access Control** Policy section and select **Edit Policy**.

   The **Policy** window opens.
3. In the **Access Control** section, click the plus sign.

   You will see a list of the Layers that you can add. These are Layers that have **Multiple policies can use this layer** enabled.
4. Select the Layer.
5. Click **OK**.
6. **Publish** the session.

Pre-R80.10 Gateways: To create a Layer for URL Filtering and Application Control:

1. In SmartConsole, click **Security Policies**.
2. Right-click a Layer in the **Access Control** Policy section and select **Edit Policy**.

   The **Policy** window opens.
3. In the **Access Control** section, click the plus sign.
4. Click **New Layer**.

   The **Layer Editor** window opens and shows the **General** view.
5. Enable Application & URL Filtering on the Layer.

   a) Enter a name for the Layer.

      We recommend the name **Application**.

   b) In the **Blades** section, select **Applications & URL Filtering**.

   c) Click **OK** and the **Layer Editor** window closes.

d) Click **OK** and the **Policy** window closes.

6. **Publish** the session.

Enabling Access Control Features

Before creating the Access Control Policy, you must enable the Access Control features that you will use in the Policy.

Enable the features on the:

- Security Gateways on which you will install the Policy.
- Ordered Layers and Inline Layers of the Policy. Here you can enable:
  - Firewall. This includes VPN ("VPN Column" on page 93).
  - Applications & URL Filtering ("Services & Applications Column" on page 94)
  - Content Awareness ("Content Column" on page 97)
  - Mobile Access ("Mobile Access to the Network" on page 94)

Enabling Access Control Features on a Gateway

1. In SmartConsole, go to **Gateways & Servers** and double-click the gateway object.
   The **General Properties** window of the gateway opens.
2. From the navigation tree, click **General Properties**.
3. In the **Network Security** tab, select one or more of these Access Control features:
   - **IPsec VPN**
   - **Mobile Access**
   - **Application Control**
   - **URL Filtering**
   - **Content Awareness**
   - **Identity Awareness**
4. Click **OK**.

Enabling Access Control Features on a Layer

To enable the Access Control features on an Ordered Layer:

1. In SmartConsole, click **Security Policies**.
2. Under **Access Control**, right-click **Policy** and select **Edit Policy**.
3. Click options  for the Layer.
4. Click **Edit Layer**.
   The **Layer Editor** window opens and shows the **General** view.
5. Enable the **Blades** that you will use in the Ordered Layer:
   - **Firewall.**
   - **Applications & URL Filtering**
   - **Content Awareness**
   - **Mobile Access**
6. Click **OK**.

To enable the Access Control features on an Inline Layer:

1. In SmartConsole, click **Security Policies**.
2. Select the Ordered Layer.
3. In the parent rule of the Inline Layer, right-click the **Action** column, and select **Inline Layer** > **Edit Layer.**
4. Enable the **Blades** that you will use in the Inline Layer:
   - **Firewall.**
   - **Applications & URL Filtering**
   - **Content Awareness**
   - **Mobile Access**

   Note - Do not enable a Blade that is not enabled in the Ordered Layer.
5. Click **OK**.

Types of Rules in the Rule Base

There are three types of rules in the Rule Base - **explicit**, **implied** and **implicit**.

Explicit rules

The rules that the administrator configures explicitly, to allow or to block traffic based on specified criteria.

Important - The **default Cleanup rule** is an explicit rule that is added by default to every new layer. You can change or delete the default Cleanup rule. We recommend that you have an explicit Cleanup rule as the last rule in each layer.

Implied rules

The default rules that are available as part of the **Global properties** configuration and cannot be edited. You can only select the implied rules and configure their position in the Rule Base:

- **First** - Applied first, before all other rules in the Rule Base - explicit or implied
- **Last** - Applied last, after all other rules in the Rule Base - explicit or implied, but before the **Implicit Cleanup Rule**
- **Before Last** - Applied before the last explicit rule in the Rule Base

Implied rules are configured to allow connections for different services that the Security Gateway uses. For example, the **Accept Control Connections** rules allow packets that control these services:

- Installation of the security policy on a Security Gateway
- Sending logs from a Security Gateway to the Security Management Server
- Connecting to third party application servers, such as RADIUS and TACACS authentication servers

Implicit cleanup rule

The default "catch-all" rule for the Layer that deals with traffic that does not match any explicit or implied rules in the Layer. It is made automatically when you create a Layer.

Implicit cleanup rules do not show in the Rule Base.

For R80.10 later version Security Gateways, the default implicit cleanup rule action is **Drop**. This is because most Policies have Whitelist rules (the Accept action). If the Layer has Blacklist rules (the Drop action), you can change the action of the implicit cleanup rule to **Accept** in the Layer Editor.

For R77.30 or earlier versions Security Gateways, the action of the implicit rule depends on the Ordered Layer:

- **Drop** - for the **Network** Layer
- **Accept** - for a Layer with **Applications and URL Filtering** enabled

Note - If you change the default values, the policy installation will fail on R77.30 or earlier versions Security Gateways.

Order in which the Firewall Applies the Rules

1. **First Implied Rule** - No explicit rules can be placed before it.
2. **Explicit Rules** - These are the rules that you create.
3. **Before Last Implied Rules** - Applied before the last explicit rule.
4. **Last Explicit Rule** - We recommend that you use a **Cleanup rule** as the last explicit rule.

   Note - If you use the **Cleanup rule** as the last explicit rule, the **Last Implied Rule** and the **Implicit Cleanup Rule** are not enforced.
5. **Last Implied Rule** - Remember that although this rule is applied after all other explicit and implied rules, the Implicit Cleanup Rule is still applied last.
6. **Implicit Cleanup Rule** - The default rule that is applied if none of the rules in the Layer match.

Configuring the Implied Rules

Some of the implied rules are enabled by default. You can change the default configuration as necessary.

To configure the implied rules:

1. In SmartConsole, select the Access Control Policy.
2. From the toolbar above the policy, select **Actions** > **Implied Rules**.

   The **Implied Policy** window opens.
3. In the left pane, click **Configuration**.
4. Select a rule to enable it, or clear a rule to disable it.
5. For the enabled rules, select the position of the rules in the Rule Base: **First**, **Last**, or **Before Last** ("Types of Rules in the Rule Base" on page 88).
6. Click **OK** and install the policy.

Showing the Implied Rules

To see the implied rules:

In **SmartConsole**, from the **Security Policies** View, select **Actions** > **Implied Rules**.

The **Implied Policy** window opens.

It shows only the implied rules, not the explicit rules.

Configuring the Implicit Cleanup Rule

To configure the Implicit Cleanup Rule:

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.
2. In the left pane, click **Layers**.
3. Select a Layer and click **Edit**.
   The **Layer Editor** opens.
4. Click **Advanced**
5. Configure the **Implicit Cleanup Rule** to *Drop* or *Accept*.
6. Click **OK**.
7. Click **Close**.
8. **Publish** the session.

Administrators for Access Control Layers

You can create administrator accounts dedicated to the role of Access Control, with their own installation and SmartConsole Read/Write permissions.

You can also delegate ownership of different Layers to different administrators ("Configuring Permissions for Access Control Layers" on page 31).

Sharing Layers

You may need to use the same rules in different parts of a Policy, or have the same rules in multiple Policy packages.

There is no need to create the rules multiple times. Define an Ordered Layer or an Inline Layer one time, and mark it as shared. You can then reuse it in multiple Policy packages. You can reuse an Inline Layer in multiple places in an Ordered Layers, or in multiple Layers.

Best Practice - Share Ordered Layers and Inline Layers with other Policy packages when possible.

To share a Layer:

1. In SmartConsole, click **Menu** > **Manage policies and layers**.
2. In the left pane, click **Layers**.
3. **Optional**: Select **Show only Shared Layers**.
4. Select a Layer.
5. Right-click and select **Edit Layer**.
6. Configure the settings in the **Layer Editor** window.
7. Select **Multiple policies and rules can use this layer.**
8. Click **OK**.
9. Click **Close**.
10. **Publish** the session.

Visual Division of the Rule Base with Sections

To better manage a policy with a large number of rules, you can use **Sections** to divide the Rule Base into smaller, logical components. The division is only visual and does not make it possible to delegate administration of different **Sections** to different administrators.

Exporting Layer Rules to a .CSV File

You can export Layer rules to a .csv file. You can open and change the .csv file in a spreadsheet application such as Microsoft Excel.

To export Layer rules to a .csv file:

1. In SmartConsole, click **Menu** > **Manage Policies and Layers**.
   The **Manage Layers** window opens.
2. Click **Layers**.
3. Select a Layer, and then click **Actions** > **Export selected Layer**.
4. Enter a path and file name.

Managing Policies and Layers

To work with Ordered Layers and Inline Layers in the Access Control Policy, select **Menu** > **Manage policies and layers** in SmartConsole.

The **Manage policies and layers** window shows.

To see the Layer in the policy package and their attributes:

In the **Layers** pane of the window, you can see:

- **Name** - Layer name
- **Number of Rules** - Number of rules in the Layer
- **Modifier**- The administrator who last changed the Layer configuration.
- **Last Modified -** Date the Layer was changed.
- **Show only Shared Layers** - A shared Layer has the **Multiple policies and rules can use this Layer** option selected ("Sharing Layers" on page 90).
- **Layer Details**
  - **Used in policies** - Policy packages that use the Layer
  - **Mode**:
    - **Ordered** - An Ordered Layer. In a Multi-Domain Security Management environment, it includes global rules and a placeholder for local, Domain rules.
    - **Inline** - An Inline Layer, also known as a Sub-Policy.
    - **Not in use** - A Layer that is not used in a Policy package.

To see the rules in the Layer:

1. Select a Layer.
2. Right-click and select **Open layer in policy**.

The Columns of the Access Control Rule Base

These are the columns of the rules in the Access Control policy. Not all of these are shown by default. To select a column that does not show, right-click on the header of the Rule Base, and select it.

Column	Description
No.	Rule number in the Rule Base Layer.
Hits	Number of times that connections match a rule ("Analyzing the Rule Base Hit Count" on page 111).
Name	Name that the system administrator gives this rule.
Source **Destination**	Network objects ("Source and Destination Column" on page 93) that define • Where the traffic starts • The destination of the traffic.
VPN	The VPN Community to which the rule applies ("VPN Column" on page 93).
Services & Applications	Services, Applications, Categories, and Sites ("Services & Applications Column" on page 94). If Application & URL Filtering is not enabled, only Services show.
Content	The data asset to protect, for example, credit card numbers or medical records ("Content Column" on page 97). You can set the direction of the data to Download Traffic (into the organization), Upload Traffic (out of the organization), or Any Direction.
Action	Action that is done when traffic matches the rule ("Actions Column" on page 98). Options include: Accept, Drop, Ask, Inform (UserCheck message), Inline Layer, and Reject.
Track	Tracking and logging action that is done when traffic matches the rule ("Tracking Column" on page 100).
Install On	Network objects that will get the rule(s) of the policy ("Installing the Access Control Policy" on page 110).
Time	Time period that this rule is enforced.
Comment	An optional field that lets you summarize the rule.

Source and Destination Column

In the Source and Destination columns of the Access Control Policy Rule Base, you can add Network objects including groups of all types. Here are some of the network objects you can include:

- Network
- Host
- Zones ("Predefined Security Zones" on page 64)
- Dynamic Objects
- Domain Objects
- Access Roles
- Online Services

To Learn More About Network Objects

You can add network objects ("Managing Objects" on page 53) to the **Source** and **Destination** columns of the Access Control Policy.

VPN Column

You can configure rules for Site-to-Site VPN, Remote Access VPN, and the Mobile Access portal and clients.

To make a rule for a VPN Community, add a Site-to-Site Community or a Remote Access VPN Community object to this column, or select **Any** to make the rule apply to all VPN Communities.

When you enable Mobile Access on a gateway, the gateway is automatically added to the **RemoteAccess** VPN Community. Include that Community in the **VPN** column of the rule or use **Any** to make the rule apply to Mobile Access gateways. If the gateway was removed from the VPN Community, the **VPN** column must contain **Any**.

IPsec VPN

The IPsec VPN solution lets the Security Gateway encrypt and decrypt traffic to and from other gateways and clients. Use SmartConsole to easily configure VPN connections between Security Gateways and remote devices.

For Site-to-Site Communities, you can configure Star and Mesh topologies for VPN networks, and include third-party gateways.

The VPN tunnel guarantees:

- Authenticity - Uses standard authentication methods
- Privacy - All VPN data is encrypted
- Integrity - Uses industry-standard integrity assurance methods

IKE and IPsec

The Check Point VPN solution uses these secure VPN protocols to manage encryption keys, and send encrypted packets. IKE (Internet Key Exchange) is a standard key management protocol that is used to create the VPN tunnels. IPsec is protocol that supports secure IP communications that are authenticated and encrypted on private or public networks.

Mobile Access to the Network

Check Point Mobile Access lets remote users easily and securely use the Internet to connect to internal networks. Remote users start a standard HTTPS request to the Mobile Access Security Gateway, and authenticate with one or more secure authentication methods.

The Mobile Access Portal lets mobile and remote workers connect easily and securely to critical resources over the internet. Check Point Mobile Apps enable secure encrypted communication from unmanaged smartphones and tablets to your corporate resources. Access can include internal apps, email, calendar, and contacts.

To include access to Mobile Access applications in the Rule Base, include the **Mobile Application** in the **Services & Applications** column.

To give access to resources through specified remote access clients, create Access Roles for the clients and include them in the **Source** column of a rule.

To Learn More About VPN

To learn more about Site-to-Site VPN and Remote Access VPN, see these guides:

- *R80.10 Site-to-Site VPN Administration Guide*
  http://downloads.checkpoint.com/dc/download.htm?ID=53104
- *R80.10 Remote Access VPN Administration Guide*
  http://downloads.checkpoint.com/dc/download.htm?ID=53105
- *R80.10 Mobile Access Administration Guide*
  http://downloads.checkpoint.com/dc/download.htm?ID=53103

Services & Applications Column

In the **Services & Applications** column of the Access Control Rule Base, define the applications, sites, and services that are included in the rule. A rule can contain one or more:

- Services
- Applications
- Mobile Applications for Mobile Access
- Web sites
- Default categories of Internet traffic
- Custom groups or categories that you create, that are not included in the Check Point Application Database.

Service Matching

The Firewall identifies (*matches*) a service according to *IP protocol*, TCP and UDP *port number*, and *protocol signature*.

To make it possible for the Firewall to match services by protocol signature, you must enable **Applications and URL Filtering** on the Gateway and on the Ordered Layer ("Enabling Access Control Features" on page 87).

You can configure TCP and UDP services to be matched by *source port*.

Application Matching

If an application is *allowed* in the policy, the rule is matched only on the **Recommended** services of the application. This default setting is more secure than allowing the application on all services. For example: a rule that allows Facebook, allows it only on the Application Control **Web Browsing Services**: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`.

If an application is *blocked* in the policy, it is blocked on all services. It is therefore blocked on all ports.

You can change the default match settings for applications.

Configuring Matching for an Allowed Application

You can configure how a rule matches an application or category that is *allowed* in the policy. You can configure the rule to match the application in one of these ways:

- On any service
- On a specified service

To do this, change the **Match Settings** of the application or category. The application or category is changed everywhere that it is used in the policy.

To change the matched services for an allowed application or category:

1. In a rule which has applications or categories in the **Services & Applications** column, double-click an application or category.
2. Select **Match Settings**.
3. Select an option:
   - The default is **Recommended** services. The defaults for Web services are the Application Control **Web Browsing Services**.
   - To match the application with all services, click **Any**.
   - To match the application on specified services, click **Customize**, and add or remove services.
   - To match the application with all services and exclude specified services, click **Customize**, add the services to exclude, and select **Negate**.
4. Click **OK**.

Configuring Matching for Blocked Applications

By default, if an application is *blocked* in the policy, it is blocked on all services. It is therefore blocked on all ports.

You can configure the matching for blocked applications so that they are matched on the recommended services. For Web applications, the recommended services are the *Application Control Web browsing services*.

If the match settings of the application are configured to **Customize**, the blocked application is matched on the customized services service. *It is not matched on all ports.*

To configure matching for blocked applications:

1. In SmartConsole, go to **Manage & Settings** > **Blades** > **Application & URL Filtering** > **Advanced Settings** > **Application Port Match**
2. Configure **Match application on 'Any' port when used in 'Block' rule**:
   - Selected - This is the default. If an application is *blocked* in the Rule Base, the application is matched to *Any* port.
   - Not selected - If an application is *blocked* in the Rule Base, the application is matched to the services that are configured in the application object of the application. However, some applications are still matched on Any. These are applications (Skype, for example) that do not limit themselves to a standard set of services.

Summary of Application Matching in a "Block" Rule

Application - Match Setting	Checkbox: Match web application on 'Any' port when used in 'Block' rule	Blocked Application is Matched on Service
Recommended services (default)	Selected (default)	Any
Recommended services (default)	Not selected	Recommended services
Customize	*Not relevant*	Customized
Any	*Not relevant*	Any

Adding Services, Applications, and Sites to a rule

You can add services, applications and sites to a rule.

Note - Rules with applications or categories do not apply to connections from or to the Security Gateway.

To add services, applications or sites to a rule:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. To add applications to a rule, select a Layer with **Applications and URL Filtering** enabled.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.
4. Search for the services, sites, applications, or categories.
5. Click the **+** next to the ones you want to add.

Creating Custom Applications, Categories, and Groups

You can create custom applications, categories or groups, that are not included in the Check Point Application Database.

To create a new application or site:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Select a Layer with **Applications and URL Filtering** enabled.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.

The Application viewer window opens.

4. Click **New > Custom Applications/Site** > **Application/Site**.
5. Enter a name for the object.
6. Enter one or more URLs.

   If you used a regular expression in the URL, click **URLs are defined as Regular Expressions**.

   Note - If the application or site URL is defined as a regular expression you must use the correct syntax.
7. Click **OK**.

To create a custom category:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Select a Layer with **Applications and URL Filtering** enabled.
3. Right-click the **Services & Applications** cell for the rule and select **Add New Items**.

   The Application viewer window opens.
4. Click **New > Custom Applications/Site** > **User Category**.
5. Enter a name for the object.
6. Enter a description for the object.
7. Click **OK**.

Services and Applications on R80 and Lower Gateways, and after Upgrade

For R77.xx and lower Gateways:

- The Firewall matches TCP and UDP services by *port* number. The Firewall cannot match services by protocol signature.
- The Firewall matches applications by the application signature.

When you upgrade the Security Management Server and the Gateway to R80 and higher, this change of behavior occurs:

- Applications that were defined in the Application & URL Filtering Rule Base are accepted on their recommended ports

Content Column

You can add Data Types to the Content column of rules in the Access Control Policy.

To use the Content column, you must enable **Content Awareness**, in the General Properties page of the Security Gateway, and on the Layer.

A Data Type is a classification of data. The Firewall classifies incoming and outgoing traffic according to Data Types, and enforces the Policy accordingly.

You can set the direction of the data in the Policy to **Download Traffic** (into the organization), **Upload Traffic** (out of the organization), or **Any Direction**.

There are two kinds of Data Types: *Content Types* (classified by analyzing the file content) and *File Types* (classified by analyzing the file ID).

Content Type examples:

- PCI - credit card numbers
- HIPAA - Medical Records Number - MRN

- International Bank Account Numbers - IBAN
- Source Code - JAVA
- U.S. Social Security Numbers - According to SSA
- Salary Survey Terms

File type examples:

- Viewer File - PDF
- Executable file
- Database file
- Document file
- Presentation file
- Spreadsheet file

Note these limitations:

- Websocket content is not inspected.
- HTTP connections that are not RFC-compliant are not inspected.

To learn more about the Data Types, open the Data Type object in SmartConsole and press the **?** button (or **F1**) to see the Help.

Note - Content Awareness and Data Loss Prevention (DLP) both use Data Types. However, they have different features and capabilities. They work independently, and the Security Gateway enforces them separately.

To learn more about DLP, see the *R80.10 Data Loss Prevention Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54805.

Actions Column

Action	Meaning
Accept	Accepts the traffic
Drop	Drops the traffic. The Firewall does not send a response to the originating end of the connection and the connection eventually does a time-out. If no UserCheck object is defined for this action, no page is displayed.
Ask	Asks the user a question and adds a confirmatory check box, or a reason box. Uses a UserCheck object.
Inform	Sends a message to the user attempting to access the application or the content. Uses a UserCheck object.

To see these actions, right-click and select **More**:

Reject	Rejects the traffic. The Firewall sends an RST packet to the originating end of the connection and the connection is closed.
UserCheck Frequency	Configure how often the user sees the configured message when the action is ask, inform, or block.

Action	Meaning
Confirm UserCheck	Select the action that triggers a UserCheck message: • **Per rule** - UserCheck message shows only once when traffic matches a rule. • **Per category** - UserCheck message shows for each matching category in a rule. • **Per application/Site** - UserCheck message shows for each matching application/site in a rule. • **Per Data type** - UserCheck message shows for each matching data type.
Limit	Limits the bandwidth that is permitted for a rule. Add a Limit object to configure a maximum throughput for uploads and downloads.
Enable Identity Captive Portal	Redirects HTTP traffic to an authentication (captive) portal. After the user is authenticated, new connections from this source are inspected without requiring authentication.

Important - A rule that drops traffic, with the **Source** and **Destination** parameters defined as **Any**, also drops traffic to and from the Captive Portal.

UserCheck Actions

UserCheck lets the Security Gateways send messages to users about possible non-compliant or dangerous Internet browsing. In the Access Control Policy, it works with URL Filtering, Application Control, and Content Awareness. (You can also use UserCheck in the Data Loss Prevention Policy, in SmartConsole). Create UserCheck objects and use them in the Rule Base, to communicate with the users. These actions use UserCheck objects:

- **Inform**
- **Ask**
- **Drop**

UserCheck on a Security Gateway

When UserCheck is enabled, the user's Internet browser shows the UserCheck messages in a new window.

You can enable UserCheck on Security Gateways that use:

- Access Control features:
  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention features:
  - Anti-Virus
  - Anti-Bot
  - Threat Emulation
  - Threat Extraction
- Data Loss Prevention

UserCheck on a computer

The UserCheck client is installed on endpoint computers. This client:

- Sends messages for applications that are not based on Internet browsers, such as Skype and iTunes, and Internet browser add-ons and plug-ins.
- Shows a message on the computer when it cannot be shown in the Internet browser.

To Learn More About UserCheck

To learn more about UserCheck, see the *R80.10 Next Generation Security Gateway Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54806.

Tracking Column

These are some of the **Tracking** options:

- **None** - Do not generate a log.
- **Log -** This is the default **Track** option. It shows all the information that the Security Gateway used to match the connection.
- **Accounting** - Select this to update the log at 10 minute intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.

To Learn More About Tracking

To learn more about Tracking options, see the *R80.20.M1 Logging and Monitoring Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_LoggingAndMonitoring_AdminGuide/html_frameset.htm.

Unified Rule Base Use Cases

Here are some use cases that show examples of rules that you can define for the Access Control Policy.

Use Cases In this section:

Use Case - Application Control and Content Awareness Ordered Layer

This use case shows an example unified Access Control Policy. It controls applications and content in one Ordered Layer.

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action	Track
General compliance (1)								
1	Block categories	Any	Internet	Any	Anonymizer Critical Risk	Any	Drop Block Message	Log
Block risky executables (2)								
2	Block download of executables files from uncategorized and high risk sites	InternalZone	Internet	Any	Uncategorized High Risk	Download Traffic Executable File	Drop	Log
Credit card data (3-4)								
3	Allow uploading of credit cards numbers, by finance, and only over HTTPS	Finance (Access Role)	Web Servers	Any	https	Upload Traffic PCI – Credit Card Numbers	Accept	Log
4	Block other credit cards from company Web servers	Any	Web Servers	Any	Any	Any Direction PCI – Credit Card Numbers	Drop	Log
Inform about sensitive data over VPN (5)								
5	Inform the user about sensitive data from VPN sites	Any	Any	RemoteAccess	Any	Any Direction Salary Survey Report	Inform	Log
cleanup (6)								
6	Cleanup rule	Any	Any	Any	Any	Any	Accept	Log

Rule	Explanation
1	**General Compliance** section **-** Block access to unacceptable Web sites and applications.
2	**Block risky executables** section - Block downloading of high risk executable files.
3-4	**Credit card data** section **-** Allow uploading of credit cards numbers only by the finance department, and only over HTTPS. Block other credit cards.
5	**Block sensitive data over VPN** section - A remote user that connects over the organization's VPN sees an informational message.
6	**cleanup rule** - Accept all traffic that does not match one of the earlier rules.

Use Case - Inline Layer for Web Traffic

This use case shows an example Access Control Policy that controls Web traffic. The Web server rules are in an Inline Layer.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
1	Headquarter WEB traffic - via proxy	HQ	Proxy	Web Proxy	Any	Ask Web Access Policy Access Noti... once a day per applic...	Log
2	Allow Proxy to the Internet	Proxy	Internet	Web	Any	Accept	None
3	Allow local branch to access the internet directly	Local Branch	Internet	Web	Any	Ask Web Access Policy Access Noti... once a day per applic...	Log
4	Web Servers	InternalZone	Web Servers	Web	Any	Web Servers protection	N/A
4.1	Block browsing with unapproved browsers	Any	Any	NEGATED Google Chrome Internet Explorer 11 Firefox Safari	Any	Drop	Log
4.2	Inform user when uploading Credit Cards only over HTTPS	Any	Any	https	Upload Traffic PCI - Credit Card Numbers	Inform Access Noti... once a day per applic...	Log
4.3	Block Credit Cards	Any	Any	Any	Any Direction PCI - Credit Card Numbers	Drop Block Message	Log
4.4	Block downloading of sensitive content	Any	Any	Any	Download Traffic HIPAA - Medical Record Headers	Drop	Log
4.5	Cleanup rule	Any	Any	Any	Any	Accept	None

No	Name	Source	Destination	Services & Applications	Content	Action	Track
5	Ask user when sending credit cards to PayPal	InternalZone	Internet	PayPal	Any Direction PCI - Credit Card Numbers	Ask Company Policy Access Noti... once a day per applic...	Log
6	Cleanup rule	Any	Any	Any	Any	Drop	Log

Rule	Explanation
4	This is the parent rule of the Inline Layer. The **Action** is the name of the Inline Layer. If a packet matches on the parent rule, the matching continues to rule 4.1 of the Inline Layer. If a packet does not match on the parent rule, the matching continues to rule 5.
4.1 -4.4	If a packet matches on rule 4.1, the rule action is done on the packet, and no more rule matching is done. If a packet does not match on rule 4.1, continue to rule 4.2. The same logic applies to the remaining rules in the Inline Layer.
4.5	If none of the higher rules in the Ordered Layer match the packet, the explicit *Cleanup Rule* is applied. The *Cleanup rule* is a default explicit rule. You can change or delete it. We recommend that you have an explicit cleanup rule as the last rule in each Inline Layer and Ordered Layer.

Use Case - Content Awareness Ordered Layer

This use case shows a Policy that controls the upload and download of data from and to the organization.

There is an explanation of some of the rules below the Rule Base.

No	Name	Source	Destination	Services & Applications	Content	Action	Track
Regulatory compliance							
1	Block the download of executable files	InternalZone	Internet	Any	Download Traffic Executable file	Drop	Log
2	Allow uploading of credit cards numbers by finance users, only over HTTPS	Finance (Access Role)	Web Servers	https	Upload Traffic PCI – Credit Card Numbers	Accept	Log
3	Block other credit cards from company Web servers	InternalZone	Web Servers	Any	Any Direction PCI – Credit Card Numbers	Drop Block Message	Log
Personally Identifiable Information							
4	Matches U.S. Social Security Numbers (SSN) allocated by the U.S. Social Security Administration (SSA).	InternalZone	Internet	Any	Upload Traffic U.S. Social Security Numbers - According to SSA	Inform Access Notifi... once a day per applicati...	Log

5	Block downloading of sensitive medical information	InternalZone	Internet	Any	Download Traffic HIPAA – Medical Records Headers	Drop Block Message	Log
Human Resources							
6	Ask user when uploading documents containing salary survey reports.	InternalZone	Internet	Any	Upload Traffic Salary Survey Report	Ask Company Policy once a day per applicati...	Log
Intellectual Property							
7	Matches data containing source code	InternalZone	Internet	Any	Any Direction Source Code	Restrict source code	N/A
7.1		Any	Any	Any	Download Traffic Source Code	Accept	Log
7.2		Any	Any	Any	Upload Traffic Source Code	Ask Company Policy once a day per applicati...	Log
7.3	Cleanup Inline Layer	Any	Any	Any	Any	Drop Block Message	Log

Rule	Explanation
1-3	**Regulatory Compliance** section **-** Control the upload and download of executable files and credit cards. You can set the direction of the **Content**. In rule 1 it is **Download Traffic**, in rule 2 it is **Upload Traffic**, and in rule 3 it is **Any Direction**. Rule 1 controls executable files, which are File Types. The File Type rule is higher in the Rule Base than rules with Content Types (Rules 2 to 7). This improves the efficiency of the Rule Base, because File Types are matched sooner than Content Types.
4-5	**Personally Identifiable Information** section - Controls the upload and download of social security number and medical records. The rule Action for rule 4 is **Inform**. When an internal user uploads a file with a social security number, the user sees a message.
6	**Human resources** section **-** controls the sending of salary survey information outside of the organization. The rule action is **Ask.** If sensitive content is detected, the user must confirm that the upload complies with the organization's policy.
7	**Intellectual Property** section - A group of rules that control how source code leaves the organization. Rule 7 is the parent rule of an Inline Layer ("Ordered Layers and Inline Layers" on page 83). The **Action** is the name of the Inline Layer. If a packet matches on rule 7.1, matching stops. If a packet does not match on rule 7.1, continue to rule 7.2. In a similar way, if there is no match, continue to 7.3. The matching stops on the last rule of the Inline Layer. We recommend that you have an explicit cleanup rule as the last rule in each Inline Layer

Use Case - Application & URL Filtering Ordered Layer

This use case shows some examples of URL Filtering and Application Control rules for a typical policy that monitors and controls Internet browsing. (The **Hits, VPN** and **Install On** columns are not shown.)

No.	Name	Source	Destination	Services & Applications	Action	Track	Time
1	Liability sites	Any	Internet	Potential liability (group)	Drop Blocked Message	Log	Any
2	High risk applications	Any	Internet	High Risk iTunes Anonymizer (category)	Drop Blocked Message	Log	Any
3	Allow IT department Remote Admin	IT (Access Role)	Any	Radmin	Allow	Log	Work-Hours
4	Allow Facebook for HR	HR(Access Role)	Internet	Facebook	Allow Download_1Gbps	Log	Any
5	Block these categories	Any	Internet	Streaming Media Protocols Social Networking P2P File Sharing Remote Administration	Drop Blocked Message	Log	Any
6	Log all applications	Any	Internet	Any	Allow	Log	Any

Rule	Explanation
1	**Liability sites**- Blocks traffic to sites and applications in the custom *Potential_liability* group. The UserCheck *Blocked Message* is shown to users and explains why their traffic is blocked.
2	**High risk applications** - Blocks traffic to sites and applications in the *High Risk* category and blocks the *iTunes* application. The UserCheck *Block Message* is shown to users and explains why their traffic is blocked.
3	**Allow IT department Remote Admin** - Allows the computers in the `IT` department network to use the *Radmin* application. Traffic that uses *Radmin* is allowed only during the *Work-Hours* (set to 8:00 through 18:30, for example).
4	**Allow Facebook for HR** - Allows computers in the HR network to use *Facebook*. The total traffic downloaded from *Facebook* is limited to 1 Gbps, there is no upload limit.
5	**Block these categories** - Blocks traffic to these categories: *Streaming Media*, *Social Networking*, *P2P File Sharing*, and *Remote Administration*. The UserCheck *Blocked Message* is shown to users and explains why their traffic is blocked. **Note** - The *Remote Administration* category blocks traffic that uses the `Radmin` application. If this rule is placed before rule 3, then this rule can also block *Radmin* for the IT department.

Rule	Explanation
6	**Log all applications**- Logs all traffic that matches any of the URL Filtering and Application Control categories.

Rule Matching in the Access Control Policy

The Firewall determines the rule to apply to a connection. This is called *matching* a connection. Understanding how the firewall matches connections will help you:

- Get better performance from the Rule Base.
- Understand the logs that show a matched connection.

Examples of Rule Matching

These example Rule Bases show how the Firewall matches connections.

Note that these Rule Bases intentionally do not follow *Best Practices for Access Control Rules* (on page 109) . This is to make the explanations of rule matching clearer.

Rule Base Matching - Example 1

For this Rule Base:

No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	ftp-pasv	Download executable file	Drop
2	Any	Any	Any	Executable file	Accept
3	Any	Any	Gambling (Category)	Any	Drop
4	Any	Any	Any	Any	Accept

This is the matching procedure for an FTP connection:

Part of connection	Firewall action	Inspection result
SYN	Run the Rule Base: Look for the first rule that matches: • Rule 1 – Match.	Final match (drop on rule 1). Shows in the log. The Firewall does not turn on the inspection engines for the other rules.

Rule Base Matching - Example 2

For this Rule Base:

No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	Any	Download executable file	Drop
2	Any	Any	Gambling (category)	Any	Drop

No.	Source	Destination	Services & Applications	Content	Action
3	Any	Any	ftp	Any	Drop
4	Any	Any	Any	Any	Accept

This is the matching procedure when browsing to a file sharing Web site. Follow the rows from top to bottom. Follow each row from left to right:

Part of connection	Firewall action	Inspection result
SYN	Run the Rule Base. Look for the first rule that matches: • Rule 1 - Possible match. • Rule 2 - Possible match. • Rule 3 - No match. • Rule 4 - Match.	Possible match (Continue to inspect the connection).
HTTP Header	The Firewall turns on inspection engines to examine the data in the connection. In this example turn on the: • URL Filtering engine – Is it a gambling site? • Content Awareness engine - Is it an executable file?	Application: File sharing (category). Content: Don't know yet.
	Optimize the Rule Base matching. Look for the first rule that matches: • Rule 1 - Possible match. • Rule 2 - No match. • Rule 3 - No match. • Rule 4 - Match.	Possible match (Continue to inspect the connection).
HTTP Body	Examine the file.	Data: PDF file.
	Optimize the Rule Base matching. Look for the first rule that matches: • Rule 1 - No match. • Rule 2 - No match. • Rule 3 - No match. • Rule 4 - Match.	Final match (accept on rule 4). Shows in the log.

Rule Base Matching - Example 3

For this Rule Base:

No.	Source	Destination	Services & Applications	Content	Action
1	InternalZone	Internet	Any	Download executable file	Drop
2	Any	Any	Gambling (Category)	Any	Drop
3	Any	Any	Any	Any	Accept

This is the matching procedure when downloading an executable file from a business Web site. Follow the rows from top to bottom. Follow each row from left to right:

Part of connection	Firewall action	Inspection result
SYN	Run the Rule Base. Look for the first rule that matches: • Rule 1 – Possible match. • Rule 2 – Possible match. • Rule 3 – Match.	Possible match (Continue to inspect the connection).
HTTP Header	The Firewall turns on inspection engines to examine the content in the connection. In this example turn on the: • URL Filtering engine – Is it a gambling site? • Content Awareness engine - Is it an executable file?	Application: Business (Category). Content: Don't know yet.
	Optimize the Rule Base matching. Look for the first rule that matches: • Rule 1 – Possible match. • Rule 2 – No match. • Rule 3 – Match.	Possible match (Continue to inspect the connection).
HTTP Body	Examine the file.	Content: Executable file.
	Optimize the Rule Base matching. Look for the first rule that matches: • Rule 1 – Match. • Rule 2 – No match. • Rule 3 – Match.	Final match (accept on rule 1). Shows in the log.

The matching examples show that:

- The Firewall sometimes runs the Rule Base more than one time. Each time it runs, the Firewall optimizes the matching, to find the first rule that applies to the connection.
- If the rule includes an application, or a site, or a service with a protocol signature (in the **Application and Services** column), or a Data Type (in the **Content** column), the Firewall:
  - Turns on one or more inspection engines.
  - Postpones making the final match decision until it has inspected the body of the connection.
- The Firewall searches for the first rule that applies to (*matches*) a connection. If the Firewall does not have all the information it needs to identify the matching rule, it continues to inspect the traffic.

Best Practices for Access Control Rules

1. Make sure you have these rules:
   - Stealth rule that prevents direct access to the Security Gateway
   - Cleanup rule that drops all traffic that is not allowed by the earlier rules in the policy.
2. Use Layers to add structure and hierarchy of rules in the Rule Base.
3. Add all rules that are based only on source and destination IP addresses and ports, in a Firewall/Network Ordered Layer at the top of the Rule Base.
4. Create Firewall/Network rules to explicitly accept safe traffic, and add an e*xplicit cleanup rule* at the bottom of the Ordered Layer to drop everything else.
5. Create an Application Control Ordered Layer after the Firewall/Network Ordered Layer. Add rules to explicitly drop unwanted or unsafe traffic. Add an explicit cleanup rule at the bottom of the Ordered Layer to accept everything else.

   Alternatively, put Application Control rules in an Inline Layer as part of the Firewall/Network rules. In the parent rule of the Inline Layer, define the Source and Destination.
6. For R80.10 Gateways and higher: If you have one Ordered Layer for Firewall/Network rules, and another Ordered Layer for Application Control - Add all rules that examine applications, Data Type, or Mobile Access elements, to the Application Control Ordered Layer, or to an Ordered Layer after it.
7. Turn off XFF inspection, unless the gateway is behind a proxy server. For more, see: sk92839 http://supportcontent.checkpoint.com/solutions?id=sk92839.
8. Disable a rule when working on it. Enable the rule when you want to use it. Disabled rules do not affect the performance of the Gateway. To disable a rule, right click in the **No.** column of the rule and select **Disable**.

Best Practices for Efficient rule Matching

1. Place rules that check the source, destination, and port (network rules) higher in the Rule Base.

   Reason: Network rules are matched sooner, and turn on fewer inspection engines.
2. Place rules that check applications and content (Data Types) below network rules.

3. Do not define a rule with *Any* in the Source and in the Destination, and with an Application or a Data Type. For example these rules are not recommended:

Source	Destination	Services & Applications	Content
Any	Any	Facebook	
Any	Any		Credit Card numbers

Instead, define one of these recommended rules:

Source	Destination	Services & Applications	Content
Any	Internet	Facebook	
Any	Server		Credit Card numbers

Reason for 2 and 3: Application Control and Content Awareness rules require content inspection. Therefore, they:

- Allow the connection until the Firewall has inspected connection header and body.
- May affect performance.

4. For rules with Data Types ("Content Column" on page 97): Place rules that check File Types higher in the Rule Base than rules that check for Content Types.

   Reason: File Types are matched sooner than Content Types.

To see examples of some of these best practices, see the Unified Rule Base Use Cases (on page 101) and Creating a Basic Access Control Policy (on page 75).

Installing the Access Control Policy

1. On the Global Toolbar, click **Menu** > **Install Policy**.

   The **Install Policy** window opens showing the Security Gateways.
2. If there is more than one Policy package: From the **Policy** drop-down list, select a policy package.
3. Select **Access Control**. You can also select other Policies.
4. If there is more than one gateway: Select the gateways on which to install the Policy.
5. Select the **Install Mode**:
   - **Install on each selected gateway independently** - Install the policy on each target gateway independently of others, so that if the installation fails on one of them, it doesn't affect the installation on the rest of the target gateways.

     Note - If you select **For Gateway Clusters, if installation on a cluster member fails, do not install on that cluster**, the Security Management Server makes sure that it can install the policy on all cluster members before it begins the installation. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all the target gateways. If the policy fails to install on one of the gateways, the policy is not installed on other target gateways.
6. Click **Install**.

Analyzing the Rule Base Hit Count

Use the Hit Count feature to show the number of connections that each rule matches. Use the Hit Count data to:

- Analyze a Rule Base - You can delete rules that have no matching connections

  Note - If you see a rule with a zero hit count it only means that in the Security Gateways enabled with Hit Count there were no matching connections. There can be matching connections on other Security Gateways.

- Better understand the behavior of the Access Control Policy

You can show Hit Count for the rules in these options:

- The percentage of the rule hits from total hits
- The indicator level (very high, high, medium, low, or zero)

These options are configured in the Access Control Policy Rule Base and also changes how Hit Count is shown in other supported Software Blades.

When you enable Hit Count, the Security Management Server collects the data from supported Security Gateways (from version R75.40 and up). Hit Count works independently from logging and tracks the hits even if the **Track** option is **None**.

Enabling or Disabling Hit Count

By default, Hit Count is globally enabled for all supported Security Gateways (from R75.40). The timeframe setting that defines the data collection time range is configured globally. If necessary, you can disable Hit Count for one or more Security Gateways.

After you enable or disable Hit Count you must install the Policy for the Security Gateway to start or stop collecting data.

To enable or disable Hit Count globally:

1. In SmartConsole, click **Menu** > **Global properties**.
2. Select **Hit Count** from the tree.
3. Select the options:
   - **Enable Hit Count** - Select to enable or clear to disable all Security Gateways to monitor the number of connections each rule matches.
   - **Keep Hit Count data up to** - Select one of the time range options. The default is 3 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.
4. Click **OK**.
5. Install the Policy.

To enable or disable Hit Count on each Security Gateway:

1. From the **Gateway Properties** for the Security Gateway, select **Hit Count** from the navigation tree.
2. Select **Enable Hit Count** to enable the feature or clear it to disable Hit Count.
3. Click **OK**.
4. Install the Policy.

Configuring the Hit Count Display

These are the options you can configure for how matched connection data is shown in the **Hits** column:

- **Value** - Shows the number of matched hits for the rule from supported Security Gateways. Connection hits are not accumulated in the total hit count for:
  - Security Gateways that are not supported
  - Security Gateways that have disabled the hit count feature

  The values are shown with these letter abbreviations:
  - K = 1,000
  - M = 1,000,000
  - G = 1,000,000,000
  - T = 1,000,000,000,000

  For example, 259K represents 259 thousand connections and 2M represents 2 million connections.
- **Percentage -** Shows the percentage of the number of matched hits for the rule from the total number of matched connections. The percentage is rounded to a tenth of a percent.
- **Level -** The hit count level is a label for the range of hits according to the table.

  The hit count range = Maximum hit value - Minimum hit value (does not include zero hits)

Hit Count Level	Icon	Range
Zero		0 hits
Low		Less than 10 percent of the hit count range
Medium		Between 10 - 70 percent of the hit count range
High		Between 70 - 90 percent of the hit count range
Very High		Above 90 percent of the hit count range

To show the Hit Count in the Rule Base:

Right-click the heading row of the Rule Base and select **Hits**.

To configure the Hit Count in a rule:

1. Right-click the rule number of the rule.
2. Select **Hit Count** and one of these options (you can repeat this action to configure more options):
   - **Timeframe** - Select **All**, **1 day**, **7 days**, **1 month**, or **3 months**
   - **Display** - Select **Percentage**, **Value**, or **Level**

To update the Hit Count in a rule:

1. Right-click the rule number of the rule.
2. Select **Hit Count > Refresh**.

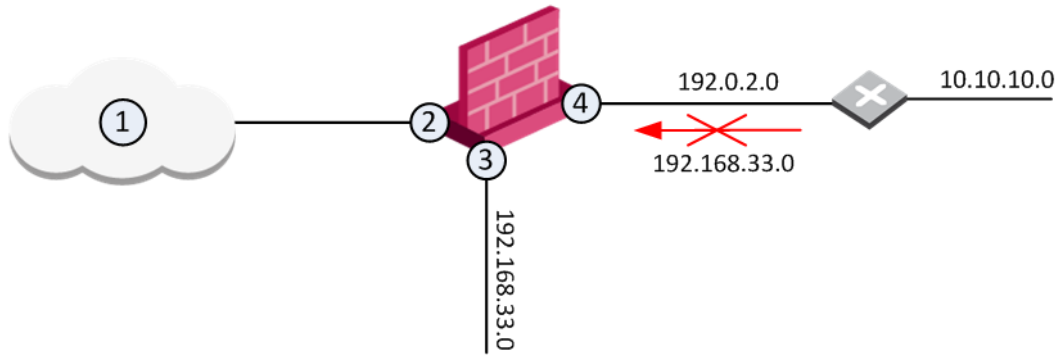
Preventing IP Spoofing

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

Anti-Spoofing detects if a packet with an IP address that is behind a certain interface, arrives from a different interface. For example, if a packet from an external network has an internal IP address, Anti-Spoofing blocks that packet.

Example:

The diagram shows a Gateway with interfaces 2 and 3, and 4, and some example networks behind the interfaces.



For the Gateway, anti-spoofing makes sure that

- All incoming packets to 2 come from the Internet (1)
- All incoming packets to 3 come from 192.168.33.0
- All incoming packets to 4 come from 192.0.2.0 or 10.10.10.0

If an incoming packet to B has a source IP address in network 192.168.33.0, the packet is blocked, because the source address is spoofed.

When you configure Anti-Spoofing protection on a Check Point Security Gateway interface, the Anti-Spoofing is done based on the interface topology. The interface topology defines where the interface **Leads To** (for example, **External** (Internet) or **Internal**), and the **Security Zone** of interface.

Configuring Anti-Spoofing

Make sure to configure Anti-Spoofing protection on all the interfaces of the Security Gateway, including internal interfaces.

To configure Anti-Spoofing for an interface:

1. In SmartConsole, go to **Gateways & Servers** and double-click the Gateway object.
   The **Gateway Properties** window opens.
2. From the navigation tree, select **Network Management**.
3. Click **Get Interfaces**.
4. Click **Accept**.
   The gateway network topology shows. If SmartConsole fails to automatically retrieve the topology, make sure that the details in the **General Properties** section are correct and the

Security Gateway, the Security Management Server, and the SmartConsole can communicate with each other.

5. Select an interface and click **Edit**.

   The interface properties window opens.

6. From the navigation tree, click **General**.

7. In the **Topology** section of the page, click **Modify**.

   The **Topology Settings** window opens.

8. In the **Leads To** section, select the type of network, to which this interface leads:

   - **Internet (External) -** This is the default setting. It is automatically calculated from the topology of the Security Gateway. To update the topology of an internal network after changes to static routes, click **Network Management** > **Get Interfaces** in the **Gateway Properties** window.
   - **Override** - Override the default setting.

   If you **Override** the default setting:

   - **Internet (External)** - All external/Internet addresses
   - **This Network (Internal)** -
     - **Not Defined** - All IP addresses behind this interface are considered a part of the internal network that connects to this interface
     - **Network defined by the interface IP and Net Mask** - Only the network that directly connects to this internal interface
     - **Network defined by routes** - The Security Gateway dynamically calculates the topology behind this interface. If the network of this interface changes, there is no need to click **Get Interfaces** and install a policy. For more, see the section *Dynamically Updating the Topology* (on page 44).
     - **Specific** - A specific object (a Network, a Host, an Address Range, or a Network Group) behind this internal interface
     - **Interface leads to DMZ** - The DMZ that directly connects to this internal interface

9. **Optional:** In the **Security Zone** section, select **User defined**, check **Specify Security Zone** and choose the zone of the interface.

10. Configure **Anti-Spoofing** options (on page 115). Make sure that **Perform Anti-Spoofing based on interface topology** is selected.

11. Select an **Anti-Spoofing action**:

    - **Prevent** - Drops spoofed packets
    - **Detect** - Allows spoofed packets. To monitor traffic and to learn about the network topology without dropping packets, select this option together with the **Spoof Tracking Log** option.

12. Configure Anti-Spoofing exceptions (optional). For example, configure addresses, from which packets are not inspected by Anti-Spoofing:

    a) Select **Don't check packets from**.

    b) Select an object from the drop-down list, or click **New** to create a new object.

13. Configure **Spoof Tracking -** select the tracking action that is done when spoofed packets are detected:

    - **Log** - Create a log entry (default)
    - **Alert** - Show an alert
    - **None** - Do not log or alert

14. Click **OK** twice to save Anti-Spoofing settings for the interface.

For each interface, repeat the configuration steps. When finished, install the Access policy.

Anti-Spoofing Options

- **Perform Anti-Spoofing based on interface topology** - Select this option to enable spoofing protection on this external interface.
- **Anti-Spoofing action is set to** - Select this option to define if packets will be rejected (the Prevent option) or whether the packets will be monitored (the Detect option). The Detect option is used for monitoring purposes and should be used in conjunction with one of the tracking options. It serves as a tool for learning the topology of a network without actually preventing packets from passing.
- **Don't check packets from** - Select this option to make sure anti-spoofing does not take place for traffic from internal networks that reaches the external interface. Define a network object that represents those internal networks with valid addresses, and from the drop-down list, select that network object. The anti-spoofing enforcement mechanism disregards objects selected in the **Don't check packets from** drop-down menu .
- **Spoof Tracking** - Select a tracking option.

Multicast Access Control

Multicast IP transmits one copy of each datagram (IP packet) to a multicast address, where each recipient in the group takes their copy. The routers in the network forward the datagrams only to routers and hosts with access to receive the multicast packets.

To configure multicast access control:

1. Open a gateway object.
2. On the **Network Management** page, select an interface and click **Edit**.
3. On **Interface** > **Advanced**, click **Drop Multicast packets by the following conditions**.
4. Select a multicast policy for the interface:
   - **Drop multicast packets whose destination is in the list**
   - **Drop all multicast packets except those whose destination is in the list**

   When access is denied to a multicast group on an interface for outbound IGMP packets, inbound packets are also denied.

   If you do not define access restrictions for multicast packets, multicast datagrams to one interface of the gateway are allowed out of all other interfaces.
5. Click **Add**.

   The **Add Object** window opens, with the **Multicast Address Ranges** object selected.
6. Click **New** > **Multicast Address Range**.

   The **Multicast Address Range Properties** window opens.
7. Enter a name for this range.
8. Define an **IP address Range** or a **Single IP Address** in the range: **224.0.0.0** - **239.255.255.255**.

   Class D IP addresses are reserved for multicast traffic and are allocated dynamically. The multicast address range `224.0.0.0` - `239.255.255.255` is used only for the destination address of IP multicast traffic.

Every IP datagram whose destination address starts with `1110` is an IP multicast datagram. The remaining 28 bits of the multicast address range identify the group to which the datagram is sent.

The `224.0.0.0 - 224.0.0.255` range is reserved for LAN applications that are never forwarded by a router. These addresses are permanent host groups. For example: an ICMP request to `224.0.0.1 is` answered by all multicast capable hosts on the network, `224.0.0.2` is answered by all routers with multicast interfaces, and `224.0.0.13` is answered by all PIM routers. To learn more, see the IANA website (http://www.iana.org/assignments/multicast-addresses).

The source address for multicast datagrams is always the unicast source address.

9. Click **OK**.
10. In the **Add Object** window, click **OK**.
11. In the **Interface Properties** window, click **OK**.
12. In the gateway window, click **OK**.
13. In the Rule Base, add a rule that allows the multicast address range as the **Destination**.
14. In the **Services** of the rule, add the multicast protocols.
    - **Multicast routing protocols** - For example: Protocol-Independent Multicast (PIM), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Extensions to OSPF (MOSPF).
    - **Dynamic registration -** Hosts use the Internet Group Management Protocol (IGMP) to let the nearest multicast router know they want to belong to a specified multicast group. Hosts can leave or join the group at any time.
15. Install the policy.

Managing Pre-R80.10 Security Gateways

When you upgrade a pre-R80 Security Management Server that manages pre-R80.10 Security Gateways to R80 or higher, the existing Access Control policies are converted in this way:

- The pre-R80 **Firewall** policy is converted into the **Network** Policy Layer of the R80 Access Control Policy. The implicit cleanup rule for it is set to **Drop** all traffic that is not matched by any rule in this Layer.
- The pre-R80 **Application & URL Filtering** policy is converted into the **Application** Policy Layer, which is the second Layer of the R80 Access Control Policy. The implicit cleanup rule for it is set to **Accept** all traffic that is not matched by any rule in this Layer.

Important – After upgrade, do not change the **Action** of the implicit cleanup rules, or the order of the Policy Layers. If you do, the policy installation will fail.

New Access Control Policy for pre-R80 Security Gateways on an R80 Security Management Server must have this structure:

1. The first Policy Layer is the Network Layer (with the **Firewall** blade enabled on it).
2. The second Policy Layer is the Application & URL Filtering Layer (with the **Application & URL Filtering** blade enabled on it).
3. There are no other Policy Layers.

If the Access Control Policy has a different structure, the policy will fail to install.

You can change the names of the Layers, for example, to make them more descriptive.

Each new Policy Layer will have the explicit default rule, added automatically and set to **Drop** all the traffic that does not match any rule in that Policy Layer. We recommend that the **Action** is set to **Drop** for the Network Policy Layer and **Accept** for the Application Control Policy Layer.

If you remove the default rule, the **Implicit Cleanup Rule** will be enforced. The **Implicit Cleanup Rule** is configured in the Policy configuration window and is not visible in the Rule Base table. Make sure the **Implicit Cleanup Rule** is configured to **Drop** the unmatched traffic for the Network Policy Layer and to **Accept** the unmatched traffic for the Application Control Policy Layer.

Configuring the NAT Policy

In This Section:

Translating IP Addresses (NAT)

NAT (Network Address Translation) is a feature of the Firewall Software Blade and replaces IPv4 and IPv6 addresses to add more security. You can enable NAT for all SmartConsole objects to help manage network traffic. NAT protects the identity of a network and does not show internal IP addresses to the Internet. You can also use NAT to supply more IPv4 addresses for the network.

The Firewall can change both the source and destination IP addresses in a packet. For example, when an internal computer sends a packet to an external computer, the Firewall translates the source IP address to a new one. The packet comes back from the external computer, the Firewall translates the new IP address back to the original IP address. The packet from the external computer goes to the correct internal computer.

SmartConsole gives you the flexibility to make necessary configurations for your network:

- Easily enable the Firewall to translate all traffic that goes to the internal network.
- SmartConsole can automatically create Static and Hide NAT rules that translate the applicable traffic.
- You can manually create NAT rules for different configurations and deployments.

How Security Gateways Translate Traffic

A Security Gateway can use these procedures to translate IP addresses in your network:

- **Static NAT** - Each internal IP address is translated to a different public IP address. The Firewall can allow external traffic to access internal resources.

  The configuration of static NAT on a *range* results in the translation of the IP addresses in the range into a *range of the same size, starting with the IP address specified.*
- **Hide NAT** - The Firewall uses port numbers to translate all specified internal IP addresses to a single public IP address and hides the internal IP structure. Connections can only start from internal computers, external computers CANNOT access internal servers. The Firewall can translate up to 50,000 connections at the same time from external computers and servers.
- **Hide NAT with Port Translation** - Use one IP address and let external users access multiple application servers in a hidden network. The Firewall uses the requested service (or destination port) to send the traffic to the correct server. A typical configuration can use these ports: FTP server (port 21), SMTP server (port 25) and an HTTP server (port 80). It is necessary to create manual NAT rules ("Automatic and Manual NAT Rules" on page 121) to use Port Translation.

Using Hide NAT

For each SmartConsole object, you can configure the IP address that is used to translate addresses for Hide NAT mode:

- Use the IP address of the external Security Gateway interface
- Enter an IP address for the object

Hide NAT uses dynamically assigned port numbers to identify the original IP addresses. There are two pools of port numbers: 600 to 1023, and 10,000 to 60,000. Port numbers are usually assigned from the second pool. The first pool is used for these services:

- `rlogin` (destination port 512)
- `rshell` (destination port 513)
- `rexec` (destination port 514)

If the connection uses one of these services, and the source port number is below 1024, then a port number is assigned from the first pool.

You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

Sample NAT Deployments

Static NAT

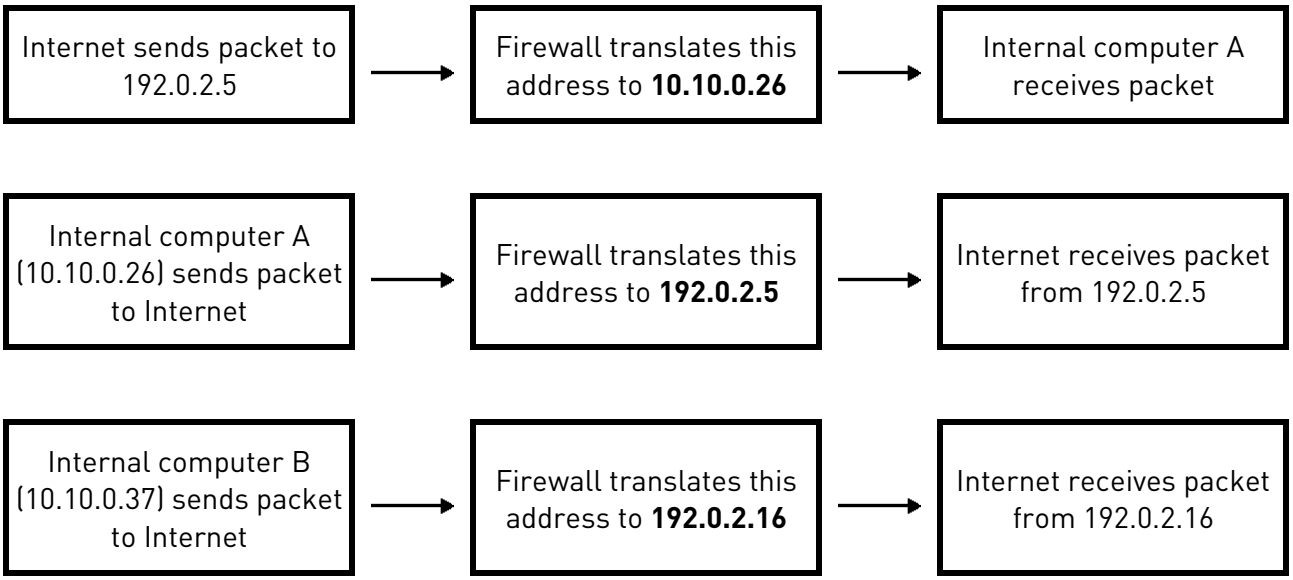
Firewalls that do Static NAT, translate each internal IP address to a different external IP address.

Item	Description
3	External computers and servers in the Internet
2	Security Gateway - Firewall is configured with Static NAT
1	Internal computers

Sample Static NAT Workflow

An external computer in the Internet sends a packet to 192.0.2.5. The Firewall translates the IP address to 10.10.0.26 and sends the packet to internal computer A. Internal computer A sends back a packet to the external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.5.

Internal computer B (10.10.0.37) sends a packet to an external computer. The Firewall intercepts the packet translates the source IP address to 192.0.2.16.



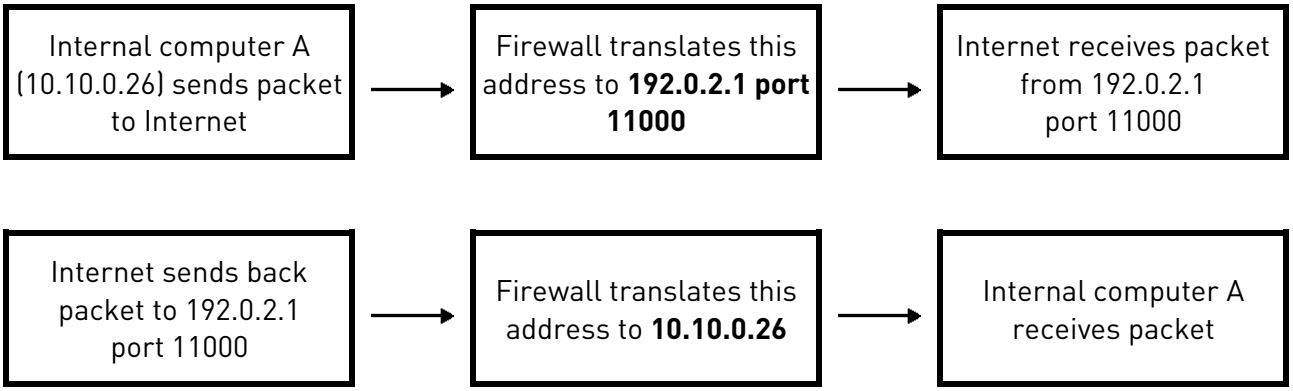
Hide NAT

Firewalls that do Hide NAT use different port numbers to translate internal IP address to one external IP address. External computers cannot start a connection to an internal computer.

Item	Description
1	Internal computers
2	Security Gateway - Firewall is configured with Hide NAT
3	External computers and servers in the Internet

Sample Hide NAT Workflow

Internal computer A (10.10.0.26) sends a packet to an external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.1 port 11000. The external computer sends back a packet to 192.0.2.1 port 11000. The Firewall translates the packet to 10.10.0.26 and sends it to internal computer A.



NAT Rule Base

The NAT Rule Base has two sections that specify how the IP addresses are translated:

- **Original Packet**
- **Translated Packet**

Each section in the NAT Rule Base is divided into cells that define the **Source**, **Destination**, and **Service** for the traffic.

Automatic and Manual NAT Rules

There are two types of NAT rules for network objects:

- Rules that SmartConsole automatically creates and adds to the NAT Rule Base
- Rules that you manually create and then add to the NAT Rule Base

When you create manual NAT rules, it can be necessary to create the translated NAT objects for the rule.

Using Automatic Rules

You can enable automatic NAT rules for these SmartConsole objects:

- Security Gateways
- Hosts
- Networks
- Address Ranges

SmartConsole creates two automatic rules for Static NAT, to translate the source and the destination of the packets.

For Hide NAT, one rule is created to translate the source of the packets.

For network and address range objects, SmartConsole creates a different rule to NOT translate intranet traffic. IP addresses for computers on the same object are not translated.

This table summarizes the NAT automatic rules:

Type of Traffic	Static NAT	Hide NAT
Internal to external	Rule translates source IP address	Rule translates source IP address
External to internal	Rule translates destination IP address	N/A (External connections are not allowed)
Intranet (for network and address range objects)	Rule does not translate IP address	Rule does not translate IP address

Order of NAT Rule Enforcement

The Firewall enforces the NAT Rule Base in a sequential manner. Automatic and manual rules are enforced differently. Automatic rules can use bidirectional NAT to let two rules be enforced for a connection.

- **Manual rules** - The first manual NAT rule that matches a connection is enforced. The Firewall does not enforce a different NAT rule that can be more applicable.
- **Automatic rules** - Two automatic NAT rules that match a connection, one rule for the **Source** and one for the **Destination** can be enforced. When a connection matches two automatic rules, those rules are enforced.

SmartConsole organizes the automatic NAT rules in this order:

1. Static NAT rules for Firewall, or host (computer or server) objects
2. Hide NAT rules for Firewall, or host objects
3. Static NAT rules for network or address range objects
4. Hide NAT rules for network or address range objects

Sample Automatic Rules

Here are some sample automatic rules.

Static NAT for a Network Object

1. Intranet connections in the HR network are not translated. The Firewall does not translate a connection between two computers that are part of the HR object.

   The Firewall does not apply rules 2 and 3 to traffic that matches rule 1.
2. Connections from IP addresses from the HR network to any IP address (usually external computers) are translated to the Static NAT IP address.
3. Connections from any IP address (usually external computers) to the HR are translated to the Static NAT IP address.

Hide NAT for Address Range

1. Intranet connections in the Sales address range are not translated. The Firewall does not translate a connection between two computers that use IP addresses that are included in the Sales object.

   The Firewall does not apply rule 2 to traffic that matches rule 1.
2. Connections from IP addresses from the Sales address range to any IP address (usually external computers) are translated to the Hide NAT IP address.

Configuring Static and Hide NAT

You can enable and configure NAT for SmartConsole objects.

Configuring Static NAT

When you enable Static NAT, each object is translated to a different IP address. SmartConsole can automatically create the NAT rules, or you can create them manually.

Configuring Hide NAT

Hide NAT uses different port numbers to identify the internal IP addresses. When you enable Hide NAT mode, the Firewall can translates the IP address to:

- The IP address of the external Security Gateway interface
- The IP address for the object

Note - You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

Enabling Automatic NAT

SmartConsole can automatically create and configure the NAT rules for a network. Enable automatic NAT for every object, for which you are translating the IP address. Then configure the Access Control Rule Base to allow traffic to the applicable objects.

To enable automatic NAT:

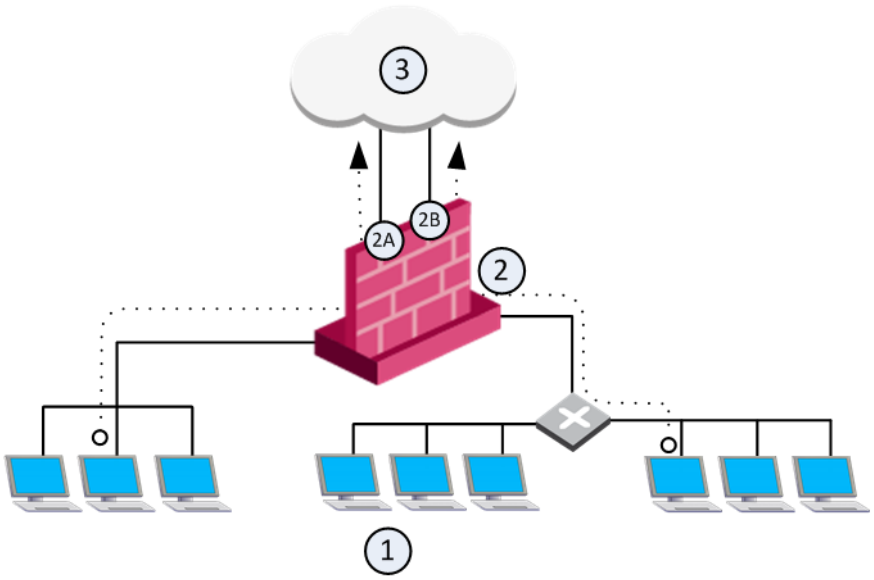
1. In SmartConsole, go to **Gateways & Servers** and double-click the gateway object.
   The **General Properties** window of the gateway opens.
2. From the navigation tree, select **NAT** > **Advanced**.
3. Select **Add automatic address translation rules to hide this Gateway behind another Gateway**.
4. Select the **Translation method**: **Hide** or **Static**.
5. Configure the NAT IP address for the object.
   - **Hide behind Gateway** - Use the IP address of the Security Gateway
   - **Hide behind IP address** - Enter the IP address.
6. Click **Install on Gateway** and select **All** or the Security Gateway that translates the IP address.
7. Click **OK**.

After you enable and configure NAT on all applicable gateways, install the policy.

Automatic Hide NAT to External Networks

For large and complex networks, it can be impractical to configure the Hide NAT settings for all the internal IP addresses. An easy alternative is to enable a Firewall to automatically Hide NAT for all traffic with external networks. The Firewall translates all traffic that goes through an external interface to the valid IP address of that interface.

In this sample configuration, computers in internal networks open connections to external servers on the Internet. The source IP addresses of internal clients are translated to the IP address of an external interface.



Item	Description
1	Internal networks
2	Security Gateway - Firewall is configured with automatic Hide NAT.
2A and 2B	Two external interfaces 192.0.2.1 and 192.0.2.100.
1 -->3	External computers and servers on the Internet

Source IP addresses are translated to the applicable external interface IP address: **192.0.2.1** or **192.0.2.100**.

Note - If a connection matches a regular NAT rule and a NAT-for-internal-networks rule, the regular NAT rule takes precedence.

To enable automatic Hide NAT:

1. In SmartConsole, go to **Gateways & Servers** and double-click the gateway object.
   The **General Properties** window of the gateway opens.
2. From the navigation tree, select **NAT**.
3. Select **Hide internal networks behind the Gateway's external IP**.
4. Click **OK**.
5. Install the policy.

Enabling Manual NAT

For some deployments, it is necessary to manually define the NAT rules. Create SmartConsole objects that use the **valid** (NATed) IP addresses. Create NAT rules to translate the original IP addresses of the objects to valid IP addresses. Then configure the Firewall Rule Base to allow traffic to the applicable translated objects with these valid IP addresses.

Note - For manual NAT rules, it is necessary to configure Proxy ARP entries to associate the translated IP address ("Automatic and Proxy ARP" on page 150).

These are some situations that must use manual NAT rules:

- Rules that are restricted to specified destination IP addresses and to specified source IP addresses
- Translate both source and destination IP addresses in the same packet.
- Static NAT in only one direction
- Translate services (destination ports)
- Rules that only use specified services (ports)
- Translate IP addresses for dynamic objects

This procedure explains how to configure manual Static NAT for a web server. You can also configure manual Hide NAT for SmartConsole objects ("Sample Deployment (Manual Rules for Port Translation)" on page 127).

To enable manual Static NAT, follow this workflow:

1. Create a clone from the network object, for example, the Web server.
2. Add a NAT rule that maps the original object to the NATed one.
3. Add Access Control rules that allow traffic to the new NATed objects.

To create a clone network object:

1. In SmartConsole, right-click the object and select **Clone**.
   The **General Properties** window of the new object opens.
2. Enter the **Name**. We recommend that you name the object **<name>_valid_address**.
3. Enter the NATed IP address.
4. Click **OK**.

To add a NAT rule to the Rule Base:

1. In SmartConsole, go to **Security Policies** > **Access Control** > **NAT**.
2. Add a manual rule above the automatic NAT rules.
3. Configure the manual rule to translate the IP address. For example:
   - **Original Source** - **WebServer**
   - **Translated Source** - **WebServer_valid_address**

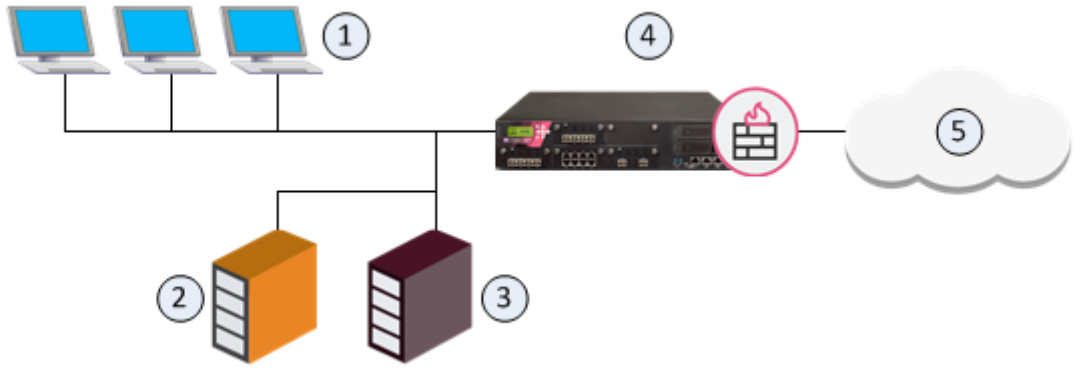
To add Access Control rules:

1. In SmartConsole, go to **Security Policies** > **Access Control** > **Policy**.
2. Add rules that allow traffic to the applicable NATed objects.
   These objects are the cloned objects that are called **<name>_valid_address**.
3. Install the policy.

Sample Deployment (Static and Hide NAT)

The goal for this sample deployment is to configure:

- Static NAT for the SMTP and the HTTP servers on the internal network. These servers can be accessed from the Internet using public addresses.
- Hide NAT for the users on the internal network that gives them Internet access. This network cannot be accessed from the Internet.



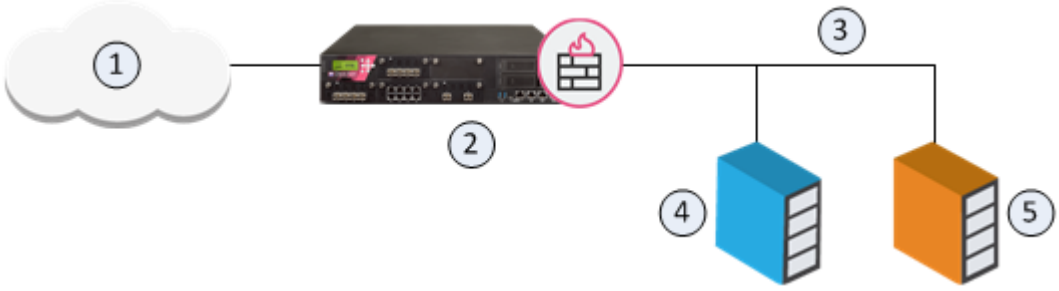
Item	Description
1	Internal computers (Alaska_LAN 2001:db8::/64)
2	Web server (Alaska.Web 2001:db8:0:10::5 translated to 2001:db8:0:a::5)
3	Mail server (Alaska.Mail 2001:db8:0:10::6 translated to 2001:db8:0:a::6)
4	Security Gateway (External interface 2001:db8:0:a::1)
5	External computers and servers in the Internet

To configure NAT for the network:

1. Enable automatic Static NAT for the web server.
   a) Double-click the Alaska.Web object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Static**.
   d) Select **Hide behind IP Address** and enter 2001:db8:0:a::5.
   e) Click **OK**.
2. Enable automatic Static NAT for the mail server.
   a) Double-click the Alaska.Mail object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Static**.
   d) Select **Hide behind IP Address** and enter 2001:db8:0:a::6.
   e) Click **OK**.
3. Enable automatic Hide NAT for the internal computers.
   a) Double-click the Alaska_LAN object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Hide**.
   d) Select **Hide behind Gateway**.
4. Click **OK** and then install the policy.

Sample Deployment (Manual Rules for Port Translation)

The goal for this sample configuration is to let external computers access a web and mail server in a DMZ network from one IP address. Configure Hide NAT for the DMZ network object and create manual NAT rules for the servers.



Item	Description
1	External computers and servers in the Internet
2	Security Gateway (Alaska_GW external interface 2001:db8:0:c::1)
3	DMZ network (Alaska_DMZ 2001:db8:a::/128)
4	Web server (Alaska_DMZ_Web 2001:db8:a::35:5 translated to 2001:db8:0:c::1)
5	Mail server (Alaska_DMZ_Mail 2001:db8:a::35:6 translated to 2001:db8:0:c::1)

To configure NAT for the DMZ servers:

1. Enable automatic Hide NAT for the DMZ network.
   a) Double-click the Alaska_DMZ object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Hide**.
   d) Select **Hide behind Gateway**.
   e) Click **OK**.
2. Create a manual NAT rule that translates HTTP traffic from the Security Gateway to the web server.
   a) In SmartConsole, go to **Security Policies** > **Access Control** > **NAT**.
   b) Add a rule below the automatic rules.
   c) Right-click the cell and select **Add new items** to configure these settings:
      - **Original Destination** - **Alaska_GW**
      - **Original Service** - **HTTP**
      - **Translated Destination** - **Alaska_DMZ_Web**
3. Create a manual NAT rule that translates SMTP traffic from the Security Gateway to the mail server.
   a) Add a rule below the automatic rules.
   b) Right-click the cell and select **Add new items** to configure these settings:
      - **Original Destination** - **Alaska_GW**

- **Original Service** - **SMTP**
- **Translated Destination** - **Alaska_DMZ_Web**

4. Create a rule in the Firewall Rule Base that allows traffic to the servers.
   a) In SmartConsole, go to **Security Policies** > **Access Control** > **NAT**.
   b) Add a rule to the Rule Base.
   c) Right-click the cell and select **Add new items** to configure these settings:
      - **Destination** - **Alaska_DMZ**
      - **Service** - **HTTP, SMTP**
      - **Action** - **Allow**
5. Install the policy.

NAT Rule Base for Manual Rules for Port Translation Sample Deployment

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	Alaska_DMZ	Alaska_DMZ	Any	Original	Original	Original	All	Automatic rule
2	Alaska_DMZ	Any	Any	H Alaska_DMZ (Hiding Address)	Original	Original	All	Automatic rule
3	Any	Alaska_GW	http	Original	S Alaska_DMZ_Web	Original	Policy Targets	
4	Any	Alaska_GW	smtp	Original	S Alaska_DMZ_Mail	Original	Policy Targets	

Configuring Stateful NAT64 (IPv6 to IPv4 translation)

R80.20.M1 supports NAT64 rules.

Background:

NAT64 translation (RFC 6146 https://tools.ietf.org/html/rfc6146) lets **IPv6-only client** communicate with **IPv4-only server** using **unicast** UDP, TCP, or ICMP.

IPv6-only client is one of these:

- A host with a networking stack that implements only IPv6.
- A host with a networking stack that implements both IPv4 and IPv6 protocols, but with only IPv6 connectivity.
- A host that runs an IPv6-only client application.

IPv4-only server is one of these:

- A host with a networking stack that implements only IPv4.
- A host with a networking stack that implements both IPv4 and IPv6 protocols, but with only IPv4 connectivity.
- A host that runs an IPv4-only server application.

The translation of IP addresses is done by translating the packet headers according to the IP/ICMP Translation Algorithm defined in RFC 6145 https://tools.ietf.org/html/rfc6145. The IPv4

addresses of IPv4 hosts are translated to and from IPv6 addresses using the algorithm defined in RFC 6052 https://tools.ietf.org/html/rfc6052, and an IPv6 prefix assigned to the stateful NAT64 for this specific purpose.

Note - For information about DNS64, see RFC 6147 https://tools.ietf.org/html/rfc6147.

Properties of Stateful NAT64:

- Performs N:M translation:
  - N must be greater than M
  - If M=1, performs a Hide NAT behind a single IPv4 address.
  - If M>1, performs a Hide NAT behind a range of IPv4 addresses.
- Gives good IPv4 address preservation (multiplexed using ports).
- Saves connection states and binding.
- There are no requirement on the assignment of IPv6 addresses to IPv6 clients. Any mode of IPv6 address assignment is legitimate (Manual, DHCP6, SLAAC).
- It is a scalable solution.

NAT64 use case scenarios:

- [IPv6 Network] --- (Internet) --- [Security Gateway] --- [internal IPv4 Network]
  Common use case for Content Providers. DNS64 is not needed.
- [internal IPv6 Network] --- [Security Gateway] --- (Internet) --- [IPv4 Network]
  Common use case for Carriers, ISPs, Enterprises. DNS64 is required.
- [IPv6 Network] --- [Security Gateway] --- [IPv4 Network]
  Common use case for Enterprises. DNS64 is required.

R80.20.M1 supports these standards for NAT64:

- RFC 6144 https://tools.ietf.org/html/rfc6146 - Framework for IPv4/IPv6 Translation
- RFC 6146 https://tools.ietf.org/html/rfc6146 - Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- RFC 6052 https://tools.ietf.org/html/rfc6052 - IPv6 Addressing of IPv4/IPv6 Translators
- RFC 6145 https://tools.ietf.org/html/rfc6145 - IP/ICMP Translation Algorithm
- RFC 2428 https://tools.ietf.org/html/rfc2428 - FTP Extensions for IPv6 and NATs
- RFC 6384 https://tools.ietf.org/html/rfc6384 - An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation

R80.20.M1 does not support these features for NAT64:

- VoIP traffic.
- HTTPS Inspection.
- SSL de-multiplexer.
- Security Gateway in HTTP Proxy mode.
- IPS protection "HTTP Header Spoofing".

Workflow for configuring NAT64 rules:

1. Prepare your Security Gateway for NAT64 ("Preparing Security Gateway for NAT64" on page 130).

2. Define the NAT64 rules ("Defining NAT64 Rules" on page 131).
3. Configure the additional settings for NAT64 ("Configuring the Additional Settings for NAT64" on page 137).

Preparing Security Gateway for NAT64

To prepare a Security Gateway for NAT64:

Note - In cluster, do these steps on *each* cluster member.

Step	Instructions
1	Make sure that an IPv6 address is assigned to the interface that connects to the destination IPv4 network, and the IPv6 network prefix length is equal to, or less than **96**. **Note -** This can be any valid IPv6 address with the IPv6 network prefix length equal to, or less than **96**. • In Gaia Portal: Click **Network Management > Network Interfaces**. • In Gaia Clish: Run: `show interface <Name of Interface> ipv6-address` If such IPv6 address is not assigned yet, assign it now. For details, see *R80.20.M1 Gaia Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_Gaia_AdminGuide/html_frameset.htm - Chapter *Network Management* - Section *Network Interfaces* - Section *Physical Interfaces*.
2	Make sure that the IPv6 routing is configured to send the traffic that is destined to the NATed IPv6 addresses (defined in the *Original Destination* column in the NAT64 rule) through the interface that connects to the destination IPv4 network. • In Gaia Portal: Click **Advanced Routing > Routing Monitor**. • In Gaia Clish: Run: `show ipv6 route` If such route does not already exist, add it in Gaia Clish. For details, see *R80.20.M1 Gaia Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_Gaia_AdminGuide/html_frameset.htm. Run these commands in Gaia Clish: 1. `set ipv6 static-route` *<NATed Destination IPv6 Addresses>/<96 or less>* `nexthop gateway` *<Any IPv6 Address from the IPv6 subnet of the Interface that connects to the destination real IPv4 network>* `on` Example topology: [IPv6 Client] --- (NATed IPv6 of IPv4 side are 1111:2222::/96) [Security Gateway] (eth3 with IPv6 3333:4444::1) --- [IPv4 Server] In such case, configure the IPv6 route using this command: `set ipv6 static-route 1111:2222::/96 nexthop gateway 3333:4444::10 on` 2. `save config`

Step	Instructions

3	Make sure that the number of IPv6 CoreXL FW instances is **equal** to the number of IPv4 CoreXL FW instances.
	1. Connect to the command line on the Security Gateway.
	2. Log in to Gaia Clish, or Expert mode.
	3. Show the number of IPv6 CoreXL FW instances. Run:
	`fw6 ctl multik stat`
	4. Show the number of IPv4 CoreXL FW instances. Run:
	`fw ctl multik stat`
	5. If the number of IPv6 CoreXL FW instances is less than the number of IPv4 CoreXL FW instances, then do these steps:
	a) Run:
	`cpconfig`
	b) Select **Check Point CoreXL**
	c) Select **Change the number of IPv6 firewall instances**
	d) Configure the number of IPv6 CoreXL FW instances to be the same as the number of IPv4 CoreXL FW instances
	e) Select **Exit**
	f) Reboot the Security Gateway
	6. Connect to the command line on the Security Gateway.
	7. Log in to Gaia Clish, or Expert mode.
	8. Show the number of IPv6 CoreXL FW instances. Run:
	`fw6 ctl multik stat`
	9. Show the number of IPv4 CoreXL FW instances. Run:
	`fw ctl multik stat`
	Example output:
	`[Expert@GW:0]# fw6 ctl multik stat`
	`ID | Active  | CPU    | Connections | Peak`
	`----------------------------------------------`
	` 0 | Yes     | 3      |           0 |        0`
	` 1 | Yes     | 2      |           0 |        4`
	` 2 | Yes     | 1      |           0 |        2`
	`[Expert@GW:0]#`
	`[Expert@GW:0]# fw ctl multik stat`
	`ID | Active  | CPU    | Connections | Peak`
	`----------------------------------------------`
	` 0 | Yes     | 3      |          10 |       14`
	` 1 | Yes     | 2      |           6 |       15`
	` 2 | Yes     | 1      |           7 |       15`
	`[Expert@GW:0]#`

Defining NAT64 Rules

Define NAT64 rules as Manual NAT rules in the Access Policy. Make sure that you add access rules that allow this NAT traffic.

Do these steps in SmartConsole to define NAT64 rules:

1. Define a source IPv6 Network object.

This object represents the source IPv6 addresses, which you translate to source IPv4 addresses.

2. Define a translated destination IPv6 Network object with an IPv4-embedded IPv6 address, or a translated destination IPv6 Host object with a static IPv6 address.

   This object represents the translated destination IPv6 address, to which the IPv6 sources connect.

3. Define a translated source IPv4 Address Range object.

   This object represents the translated source IPv4 addresses, to which you translate the original source IPv6 addresses.

4. Create a Manual NAT64 rule.
5. Install the Access Policy.

To define a source IPv6 Network object that represents the source IPv6 address, which you translate to source IPv4 addresses:

1. Click **Objects** menu **> New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

   Do not enter anything.

6. In the **IPv6** section:

   a) In the **Network address** field, enter the IPv6 address of your IPv6 network, which you translate to source IPv4 addresses.

   b) In the **Prefix** field, enter the prefix of your IPv6 network.

7. On the **NAT** page of this object:

   Do not configure anything.

8. Click **OK**.

To define a translated destination IPv6 Network object with IPv4-embedded IPv6 address that represents the IPv6 addresses, to which the IPv6 sources connect:

1. Click **Objects** menu **> New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

   Do not enter anything.

6. In the **IPv6** section:

   a) In the **Network address** field, enter the destination *IPv4-embedded* IPv6 address (also called *IPv4-mapped* IPv6 address), to which the IPv6 sources connect.

   Such IPv6 address contains (from left to right) 80 "zero" bits, followed by 16 "one" bits, and then the 32 bits of the IPv4 address - 0:0:0:0:0:FFFF:X.Y.Z.W, where X.Y.Z.W are the four octets of the destination IPv4 address.

For example, for IPv4 network 192.168.3.0, the IPv4-embedded IPv6 address is 0:0:0:0:0:FFFF:192.168.3.0, or 0:0:0:0:0:FFFF:C0A8:0300. For more information, see RFC 6052 https://tools.ietf.org/html/rfc6052.

These IPv4-embedded IPv6 addresses are published by an external DNS64 server.

b) In the **Prefix** field, enter the applicable IPv6 prefix.

Note - You can define IPv4-embedded IPv6 addresses only for these object types: Address Range, Network, and Host.

7. On the **NAT** page of this object:

   Do not configure anything.

8. Click **OK**.

To define a translated destination IPv6 Host object with static IPv6 address that represents the IPv6 address, to which the IPv6 sources connect:

1. Click **Objects** menu **> New Host**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

   Do not enter anything.

6. In the **IPv6** section:

   In the **Network address** field, enter the destination static IPv6 address, to which the IPv6 sources connect.

7. On the **NAT** page of this object:

   Do not configure anything.

8. Configure the applicable settings on other pages of this object.
9. Click **OK**.

To define a translated source IPv4 Address Range object that represents the IPv4 addresses, to which you translate the source IPv6 addresses:

1. Click **Objects** menu **> More object types > Network Object > Address Range > New Address Range**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

   a) In the **First IP address** field, enter the first IPv4 address of your IPv4 addresses range, to which you translate the source IPv6 addresses.

   b) In the **Last IP address** field, enter the last IPv4 address of your IPv4 addresses range, to which you translate the source IPv6 addresses.

   Notes:

   - This IPv4 addresses range must not use private IPv4 addresses (see RFC 1918 https://tools.ietf.org/html/rfc1918 and **Menu > Global properties > Non Unique IP Address Range**).
   - This IPv4 addresses range must not be used on the IPv4 side of the network.

- We recommend that you define a large IPv4 addresses range for more concurrent NAT64 connections.

6. In the **IPv6** section:
   Do not enter anything.
7. On the **NAT** page of this object:
   Do not configure anything.
8. Click **OK**.

To create a Manual NAT64 rule:

1. From the left Navigation Toolbar, click **SECURITY POLICIES**.
2. In the top **Access Control** section, click **NAT**.
3. Right-click on the **Manual Lower Rules** section title, and near the **New Rule**, click **Above** or **Below**.
4. Configure this NAT64 rule:
   Important - Some combinations of object types are not supported in the *Original Source* and *Original Destination* columns. See the summary table with the supported NAT rules at the bottom of this section.

Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
***Any** or IPv6 **Host** object or IPv6 **Address Range** object or IPv6 **Network** object	IPv6 **Host** object or IPv6 **Address Range** object with an IPv4-embedded IPv6 addresses or IPv6 **Network** object with an IPv4-embedded IPv6 address	***Any**	IPv4 **Address Range** object for your translated IPv4 addresses	**Embedded IPv4 Address**	**= Original**

   Do these steps:

   a) In the **Original Source** column, add the IPv6 object for your original source IPv6 addresses.
      In this rule column, NAT64 rules support only these types of objects:
      - *Any
      - Host with a static IPv6 address
      - Address Range with IPv6 addresses
      - Network with IPv6 address

   b) In the **Original Destination** column, add a translated destination IPv6 object with an IPv4-embedded IPv6 address.

In this rule column, NAT64 rules support only these types of objects:

- Host with a static IPv6 address
- Address Range with IPv4-embedded IPv6 addresses
- Network with an IPv4-embedded IPv6 address

c) In the **Original Services** column, you must leave the default **Any**.

d) In the **Translated Source** column, add the IPv4 **Address Range** object for your translated source IPv4 addresses range.

In this rule column, NAT64 rules support only these types of objects:

- Host with a static IPv4 address, only if in the **Original Source** column you selected a Host with a static IPv6 address
- Address Range with IPv4 addresses

e) In the **Translated Source** column, right-click the IPv4 **Address Range** object > click **NAT Method** > click **Stateful NAT64**:

- The **Translated Packet Destination** column shows **= Embedded IPv4 Address**.
- The **64** icon shows in both the **Translated Source** and **Translated Destination** columns.

In this rule column, NAT64 rule supports only these types of objects:

- Host with a static IPv4 address, only if in the **Original Source** column you selected a Host with a static IPv6 address
- Embedded IPv4 Address

f) In the **Translated Services** column, you must leave the default **= Original**.

To summarize, you must configure only these NAT64 rules (rule numbers are for convenience only):

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
1	*Any	IPv6 *Host* object with a static IPv6 address	*Any	IPv4 *Address Range* object	IPv4 *Host* object	= Original
2	*Any	IPv6 *Address Range* object with an IPv4-embedded IPv6 addresses	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
3	*Any	IPv6 *Network* object with an IPv4-embedded IPv6 address	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
4	IPv6 *Host* object with a static IPv6 address	IPv6 *Host* object with a static IPv6 address	*Any	IPv4 *Host* object	IPv4 *Host* object	= Original
5	IPv6 *Host* object with a static IPv6 address	IPv6 *Address Range* object with IPv4-embedded IPv6 addresses	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
6	IPv6 *Host* object with a static IPv6 address	IPv6 *Network* object with an IPv4-embedded IPv6 address	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
7	IPv6 *Address Range* object	IPv6 *Host* object with a static IPv6 address	*Any	IPv4 *Address Range* object	IPv4 *Host* object	= Original
8	IPv6 *Address Range* object	IPv6 *Address Range* object with IPv4-embedded IPv6 addresses	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
9	IPv6 *Address Range* object	IPv6 *Network* object with an IPv4-embedded IPv6 address	*Any	IPv4 *Address Range* object	Embedded IPv4 Address	= Original
10	IPv6 *Network* object	IPv6 *Host* object with a static IPv6 address	*Any	IPv4 *Address Range* object	IPv4 *Host* object	= Original

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
11	IPv6 *Network* object	IPv6 *Address Range* object with IPv4-embedded IPv6 addresses	*Any	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`
12	IPv6 *Network* object	IPv6 *Network* object with an IPv4-embedded IPv6 address	*Any	IPv4 *Address Range* object	`Embedded IPv4 Address`	`= Original`

1. Publish the session and install the Access Policy.

Configuring the Additional Settings for NAT64

You can configure the additional settings that control the NAT64 translation mechanism. These settings are compliant with RFC 6145 https://tools.ietf.org/html/rfc6145.

Note - We recommend that you change the default settings only if you are familiar with the technology.

1. Close all SmartConsole windows.
2. Connect with GuiDBedit Tool http://supportcontent.checkpoint.com/solutions?id=sk13009 to the applicable Security Management Server or Domain Management Server.
3. In the top left section, click **Table > Global Properties > properties**.
4. In the top right section, click **firewall_properties**.
5. In the bottom section, scroll to these **Field Names**:
   - `nat64_add_UDP_checksum`
   - `nat64_avoid_PMTUD_blackhole`
   - `nat64_copy_type_of_service`
   - `nat64_error_message_on_dropped_packets`
6. Right-click on the applicable Field Name and click **Edit**.
7. Select the applicable **Value** (**true**, or **false**) and click **OK**.

Field Name	Description
`nat64_add_UDP_checksum`	This setting controls whether the translator should calculate and add a valid UDP checksum value to a packet, if the packet checksum value is zero. This is important because, by default, an IPv4 UDP packet with a checksum value of zero is dropped on the IPv6 side. **Default:** false

Field Name	Description
`nat64_avoid_PMTUD_blackhole`	This setting controls whether to allow packet fragmentation on the IPv4 (destination) side during PMTU discovery. Enable this setting if some equipment combinations cause PMTU discovery to fail. **Default:** false
`nat64_copy_type_of_service`	This setting controls whether to copy the traffic **Class Field** to the **Type Of Service** field, and set the **Type Of Service** field in the translated packet to zero. **Default:** true
`nat64_error_message_on_dropped_packets`	This setting controls whether to generate an audit log after a connection is closed. For each closed connection, the log shows: • Connection information (source and destination IP address, source port, and service). • Translated source IP address and source port. • Start time and end time. • If the connection was closed because the connection expired, log shows additional information in the **TCP End Reason** field. If this field does not show in the log, the connection was closed with a TCP RST, or with a TCP FIN, and did not expire. **Default:** true

1. Click **File > Save All** to save the changes.
2. Close the GuiDBedit Tool.
3. Connect with the SmartConsole to the applicable Security Management Server or Domain Management Server.
4. Install the Access Policy.

Logging of NAT64 traffic

In the Security Gateway log for NAT64 connection, the source and destination IPv6 addresses show in their original IPv6 format. To identify a NAT64 entry, look in the **More** section of the **Log Details** window.

Field in Log	Description
Xlate (NAT) Source IP	Shows the translated source IPv4 address, to which the Security Gateway translated the original source IPv6 address
Xlate (NAT) Destination IP	Shows the translated destination IPv4 address, to which the Security Gateway translated the original destination IPv6 address
More	Identifies the entry as NAT64 traffic (`Nat64 enabled`)

Example of NAT64 Translation Flow

Example topology:

[IPv6 Client] --- (interface) [Security Gateway] (internal) --- [IPv4 Server]

Where:

Item	Description
IPv6 Client	IPv6 real address is 1111:1111::0100/96
Security Gateway external interface	IPv6 address is 1111:1111::1/96
Security Gateway internal interface	IPv4 address is 10.0.0.1/24 IPv6 address is 3333:4444::1/96
IPv4 Server	IPv4 real address is 10.0.0.100/24 IPv6 NATed address is 1111:2222::0A00:0064/96
IPv6 NATed network	IPv6 address of the network on the external Security Gateway side is 1111:2222::/96 These IPv6 addresses are used to translate the IPv4 address of the IPv4 Server to the IPv6 address
IPv4 NATed network	IPv4 address of the network on the internal Security Gateway side is 1.1.1.0/24 These IPv4 addresses are used to translate the IPv6 address of the IPv6 Client to the IPv4 address

Traffic flow:

1. IPv6 Client opens an IPv6 connection to the NATed IPv6 address of the IPv4 Server:
   From the IPv6 Client's IPv6 real address 1111:1111::0100 to the IPv4 Server's NATed IPv6 address 1111:2222::0A00:0064
   Where:
   The "1111:2222::" part is the NATed IPv6 subnet
   The "0A00:0064" part is 10.0.0.100
2. Security Gateway performs these NAT translations:
   a) Translate the IPv6 Client's *source* address from the real IPv6 address 1111:1111::0100 to the special concatenated *source* IPv6 address 0064:FF9B::0101:01XX
      Where:
      The "0064:FF9B::" part is a well-known prefix reserved for NAT64 (as defined by the RFC)
      The "0101:01XX" part is 1.1.1.X
   b) Translate the IPv6 Client's *source* address from the special concatenated *source* IPv6 address 0064:FF9B::0101:01XX to the *source* IPv4 address 1.1.1.X
   c) Translate the IPv6 Client's NATed *destination* address from the IPv6 address 1111:2222::0A00:0064 to the NATed destination IPv4 address 10.0.0.100

3. IPv4 Server receives this request connection as from the *source* IPv4 address 1.1.1.X to the *destination* IPv4 address 10.0.0.100
4. IPv4 Server replies to this connection from the *source* IPv4 address 10.0.0.100 to the *destination* IPv4 address 1.1.1.X
5. Security Gateway performs these NAT translations:
   a) Translate the IPv4 Server's *source* real IPv4 address 10.0.0.100 to the *source* NATed IPv6 address 1111:2222::0A00:0064
   b) Translate the IPv6 Client's NATed *destination* IPv4 address 1.1.1.X to the *destination* special concatenated IPv6 address 0064:FF9B::0101:01XX

      Where:

      The "64:FF9B::" part is a well-known prefix reserved for NAT64 (as defined by the RFC)

      The "0101:01XX" part is 1.1.1.X
   c) Translate the IPv6 Client's *destination* special concatenated IPv6 address 0064:FF9B::0101:01XX to the *destination* IPv6 real address 1111:1111::0100
6. IPv6 Client receives this reply connection as from the *source* IPv6 address 1111:2222::0A00:0064 to the *destination* IPv6 address 1111:1111::0100

To summarize:

- *Request*: [IPv6 Client] ---> [Security Gateway] ---> [IPv4 Server]

Field in packet	Original IPv6 packet	NATed IPv4 packet
Source IP	1111:1111::0100 / 96	1.1.1.X / 24
Destination IP	1111:2222::0A00:0064 / 96	10.0.0.100 / 24

- *Reply*: [IPv6 Client] <--- [Security Gateway] <--- [IPv4 Server]

Field in packet	Original IPv4 packet	NATed IPv6 packet
Source IP	10.0.0.100 / 24	1111:2222::0A00:0064 / 96
Destination IP	1.1.1.X / 24	1111:1111::0100 / 96

Configuring Stateless NAT46 (IPv4 to IPv6 translation)

NAT46 rules are only supported on R80.20 gateways.

Background:

NAT46 translation lets an **IPv4** network communicate with an **IPv6** network without maintaining any session information on Security Gateway.

Properties of Stateless NAT46:

- Performs 1:1 IP address mapping.
- The system generates the translated source IPv6 address as a combination of these two parts:
  a) A user-defined Network object with an IPv6 address defined with the 96-bit prefix.
  b) The source IPv4 address, which is added as a 32-bit suffix.

NAT46 use case scenarios:

- [IPv4 Network] --- (Internet) --- [Security Gateway] --- [IPv6 Network]
  Common use case for Content Providers.
- [IPv4 Network] --- [Security Gateway] --- (Internet) --- [IPv6 Network]
  Common use case for Enterprises.

R80.20.M1 does not support these features not for NAT46:

- VoIP traffic.
- FTP traffic.
- Any protocols that require state information between Control and Data connections.

Workflow for configuring NAT46 rules:

1. Prepare your Security Gateway for NAT46 ("Preparing Security Gateway for NAT46" on page 141).
2. Define the NAT46 rules ("Defining NAT46 Rules" on page 143).

Preparing Security Gateway for NAT46

To prepare a Security Gateway for NAT46:

Note - In cluster, do these steps on *each* cluster member.

Step	Instructions
1	Make sure that an IPv6 address is assigned to the interface that connects to the destination IPv6 network, and the IPv6 network prefix length is equal to 96. **Note -** This can be any valid IPv6 address with the IPv6 network prefix length equal to **96**. • In Gaia Portal: Click **Network Management > Network Interfaces**. • In Gaia Clish: Run: `show interface <Name of Interface> ipv6-address` If such IPv6 address is not assigned yet, assign it now. For details, see *R80.20.M1 Gaia Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_Gaia_AdminGuide/html_frameset.htm - Chapter *Network Management* - Section *Network Interfaces* - Section *Physical Interfaces*.

Step	Instructions
2	Make sure that the routing is configured to send the traffic that is destined to the NATed IPv4 addresses (defined in the *Translated Destination* column in the NAT46 rule) through the interface that connects to the destination IPv6 network. • In Gaia Portal: Click **Advanced Routing > Routing Monitor**. • In Gaia Clish: Run: `show route` If such route does not already exist, add it in Gaia Clish. For details, see *R80.20.M1 Gaia Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_Gaia_AdminGuide/html_frameset.htm. Run these commands in Gaia Clish: 1. `set static route` <*NATed Destination IPv4 Addresses*>/<*NATed IPv4 Net Mask*> `nexthop gateway logical` <*Name of Interface that connects to the real IPv6 Network*> `on` Example topology: [IPv4 Client] --- (NATed IPv4 of IPv6 side are 1.1.1.0/24) [Security Gateway] (eth3) --- [IPv6 Server] In such case, configure the IPv4 route using this command: `set static route 1.1.1.0/24 nexthop gateway logical eth3 on` 2. `save config`

Step	Instructions

3	Make sure that the number of IPv6 CoreXL FW instances is **equal** to the number of IPv4 CoreXL FW instances.
	1. Connect to the command line on the Security Gateway.
	2. Log in to Gaia Clish, or Expert mode.
	3. Show the number of IPv6 CoreXL FW instances. Run:
	`fw6 ctl multik stat`
	4. Show the number of IPv4 CoreXL FW instances. Run:
	`fw ctl multik stat`
	5. If the number of IPv6 CoreXL FW instances is less than the number of IPv4 CoreXL FW instances, then do these steps:
	a) Run:
	`cpconfig`
	b) Select **Check Point CoreXL**
	c) Select **Change the number of IPv6 firewall instances**
	d) Configure the number of IPv6 CoreXL FW instances to be the same as the number of IPv4 CoreXL FW instances
	e) Select **Exit**
	f) Reboot the Security Gateway
	6. Connect to the command line on the Security Gateway.
	7. Log in to Gaia Clish, or Expert mode.
	8. Show the number of IPv6 CoreXL FW instances. Run:
	`fw6 ctl multik stat`
	9. Show the number of IPv4 CoreXL FW instances. Run:
	`fw ctl multik stat`
	Example output:
	`[Expert@GW:0]# fw6 ctl multik stat`
	`ID | Active  | CPU    | Connections | Peak`
	`----------------------------------------------`
	` 0 | Yes     | 3      |           0 |        0`
	` 1 | Yes     | 2      |           0 |        4`
	` 2 | Yes     | 1      |           0 |        2`
	`[Expert@GW:0]#`
	`[Expert@GW:0]# fw ctl multik stat`
	`ID | Active  | CPU    | Connections | Peak`
	`----------------------------------------------`
	` 0 | Yes     | 3      |          10 |       14`
	` 1 | Yes     | 2      |           6 |       15`
	` 2 | Yes     | 1      |           7 |       15`
	`[Expert@GW:0]#`

Defining NAT46 Rules

Define NAT46 rules as Manual NAT rules in the Access Policy. Make sure that you add access rules that allow this NAT traffic.

Do these steps in SmartConsole to define NAT46 rules:

1. Define an applicable source IPv4 object (IPv4 Host, IPv4 Address Range, or IPv4 Network).
2. Define a destination IPv4 Host object.

This object represents the destination IPv4 address, to which the IPv4 sources connect.

3. Define a translated source IPv6 Network object with an IPv6 address defined with the 96-bit prefix.

   This object represents the translated source IPv6 addresses, to which you translate the source IPv4 addresses.

4. Define a translated destination IPv6 Host object.

   This object represents the translated destination IPv6 address, to which the translated IPv4 sources connect.

5. Create a Manual NAT46 rule.
6. Install the Access Policy.

To define a source IPv4 Host object:

1. Click **Objects** menu **> New Host**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4 address** field, enter the source IPv4 address.
6. In the **IPv6** section:

   Do not enter anything

7. On the **NAT** page of this object:

   Do not configure anything.

8. Configure the applicable settings on other pages of this object.
9. Click **OK**.

To define a source IPv4 Network object:

1. Click **Objects** menu **> New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:

   a) In the **Network address** field, enter the IPv4 address of your source IPv4 network.

   b) In the **Net mask** field, enter the net mask of your source IPv4 network.

6. In the **IPv6** section:

   Do not enter anything.

7. On the **NAT** page of this object:

   Do not configure anything.

8. Click **OK**.

To define a source IPv4 Address Range object:

1. Click **Objects** menu **> More object types > Network Object > Address Range > New Address Range**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.

5. In the **IPv4** section:
   a) In the **First IP address** field, enter the first IPv4 address of your IPv4 addresses range.
   b) In the **Last IP address** field, enter the last IPv4 address of your IPv4 addresses range.
6. In the **IPv6** section:
   Do not enter anything.
7. On the **NAT** page of this object:
   Do not configure anything.
8. Click **OK**.

To define a translated destination IPv4 Host object:

1. Click **Objects** menu **> New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:
   a) In the **Network address** field, enter the IPv4 address of your destination IPv4 network.
   b) In the **Net mask** field, enter the net mask of your destination IPv4 network.
6. In the **IPv6** section:
   Do not enter anything.
7. On the **NAT** page of this object:
   Do not configure anything.
8. Click **OK**.

To define a translated source IPv6 Network object with an IPv6 address defined with the 96-bit prefix:

1. Click **Objects** menu **> New Network**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.
4. Click the **General** page of this object.
5. In the **IPv4** section:
   Do not enter anything.
6. In the **IPv6** section:
   a) In the **Network address** field, enter the translated source IPv6 address.
   b) In the **Prefix** field, enter the number **96**.
7. On the **NAT** page of this object:
   Do not configure anything.
8. Click **OK**.

To define a translated destination IPv6 Host object:

1. Click **Objects** menu **> New Host**.
2. In the **Object Name** field, enter the applicable name.
3. In the **Comment** field, enter the applicable text.

4. Click the **General** page of this object.
5. In the **IPv4** section:
   Do not enter anything.
6. In the **IPv6** section:
   In the **Network address** field, enter the destination static IPv6 address.
7. On the **NAT** page of this object:
   Do not configure anything.
8. Configure the applicable settings on other pages of this object.
9. Click **OK**.

To create a Manual NAT46 rule:

1. From the left Navigation Toolbar, click **SECURITY POLICIES**.
2. In the top **Access Control** section, click **NAT**.
3. Right-click on the **Manual Lower Rules** section title, and near the **New Rule**, click **Above** or **Below**.
4. Configure this NAT46 rule:

Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
***Any** or Source IPv4 **Host** object or Source IPv4 **Address Range** object or Source IPv4 **Network** object	IPv4 **Host** object	***Any**	IPv6 **Network** object with an IPv6 address defined with the 96-bit prefix	IPv6 **Host** object	**= Original**

   Do these steps:

   a) In the **Original Source** column, add the applicable IPv4 object.

      In this rule column, NAT46 rules support only these types of objects:

      - *Any
      - Host with a static IPv4 address
      - Address Range with IPv4 addresses
      - Network with IPv4 address

b) In the **Original Destination** column, add the IPv4 **Host** object that represents the destination IPv4 address, to which the IPv4 sources connect.

In this rule column, NAT46 rules support only IPv4 Host objects.

c) In the **Original Services** column, you must leave the default **Any**.

d) In the **Translated Source** column, add the IPv6 **Network objec**t with an IPv6 address defined with the 96-bit prefix.

In this rule column, NAT64 rules support only IPv6 Network objects with an IPv6 address defined with the 96-bit prefix.

e) In the **Translated Source** column, right-click the IPv6 **Network objec**t with the 96-bit prefix > click **NAT Method** > click **Stateless NAT46**.

The **46** icon shows in the **Translated Source** column.

f) In the **Translated Destination** column, add the IPv6 **Host** object represents the translated destination IPv6 address, to which the translated IPv4 sources connect.

In this rule column, NAT46 rule supports only an IPv6 Host objects.

g) In the **Translated Services** column, you must leave the default **= Original**.

To summarize, you must configure only these NAT46 rules (rule numbers are for convenience only):

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
1	*Any	IPv4 *Host* object	*Any	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	= Original
2	IPv4 *Host* object with a static IPv4 address	IPv4 *Host* object	*Any	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	= Original
3	IPv4 *Address Range* object	IPv4 *Host* object	*Any	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	= Original

#	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
4	IPv4 *Network* object	IPv4 *Host* object	*Any	IPv6 *Network* object with an IPv6 address defined with the 96-bit prefix	IPv6 *Host* object	= Original

5. Publish the session and install the Access Policy.

Logging of NAT46 traffic

In the Security Gateway log for NAT64 connection, the source and destination IPv6 addresses show in their original IPv6 format. To identify a NAT46 entry, look in the **More** section of the **Log Details** window.

Field in Log	Description
Xlate (NAT) Source IP	Shows the translated source IPv6 address, to which the Security Gateway translated the original source IPv4 address
Xlate (NAT) Destination IP	Shows the translated destination IPv6 address, to which the Security Gateway translated the original destination IPv4 address
More	Identifies the entry as NAT46 traffic (`Nat46 enabled`)

Example of NAT46 Translation Flow

Example topology:

[IPv4 Client] --- (internal) [Security Gateway] (external) --- [IPv6 Server]

Where:

Item	Description
IPv4 Client	IPv4 real address is 192.168.2.55 IPv6 NATed address is 2001:DB8:90::192.168.2.55**/96**
Security Gateway internal interface	IPv4 address is 192.168.2.1/24
Security Gateway external interface	IPv6 address is 2001:DB8:5001::1/**96**
IPv6 Server	IPv6 real address is 2001:DB8:5001::30/96 IPv4 NATed address is 1.1.1.66/24

Item	Description
IPv6 NATed network	IPv6 address of the network on the external Security Gateway side is 2001:DB8:90::/96 These IPv6 addresses are used to translate the IPv4 address of the IPv4 Client to IPv6 address
IPv4 NATed network	IPv4 address of the network on the internal Security Gateway side is 1.1.1.0/24 These IPv4 addresses are used to translate the IPv6 address of the IPv6 Server to IPv4 address

Traffic flow:

1. IPv4 Client opens an IPv4 connection to the NATed IPv4 address of the IPv6 Server
   From IPv4 address 192.168.2.55 to IPv4 address 1.1.1.66
2. Security Gateway performs these NAT translations:
   a) From the source IPv4 address 192.168.2.55 to the source IPv6 address 2001:DB8:90::192.168.2.55/96
   b) From the destination IPv4 address 1.1.1.66 to the destination IPv6 address 2001:DB8:5001::30
3. IPv6 Server receives this request connection as from the IPv6 address 2001:DB8:90::192.168.2.55/96 to the IPv6 address 2001:DB8:5001::30
4. IPv6 Server replies to this connection from the IPv6 address 2001:DB8:5001::30 to the IPv6 address 2001:DB8:90::192.168.2.55/96
5. Security Gateway performs these NAT translations:
   a) From the source IPv6 address 2001:DB8:5001::30 to the source IPv4 address 1.1.1.66
   b) From the destination IPv6 address 2001:DB8:90::192.168.2.55/96 to the destination IPv4 address 192.168.2.55
6. IPv4 Client receives this reply connection as from the IPv4 address 1.1.1.66 to the IPv4 address 192.168.2.55

To summarize:

- Request: [IPv4 Client] ---> [Security Gateway] ---> [IPv6 Server]

Field in packet	Original IPv4 packet	NATed IPv6 packet
Source IP	192.168.2.55 / 24	2001:DB8:90::192.168.2.55 / 96
Destination IP	1.1.1.66 / 24	2001:DB8:5001::30 / 96

- Reply: [IPv4 Client] <--- [Security Gateway] <--- [IPv6 Server]

Field in packet	Original IPv6 packet	NATed IPv4 packet
Source IP	2001:DB8:5001::30 / 96	192.168.2.55 / 24
Destination IP	2001:DB8:90::192.168.2.55 / 96	1.1.1.66 / 24

Advanced NAT Settings

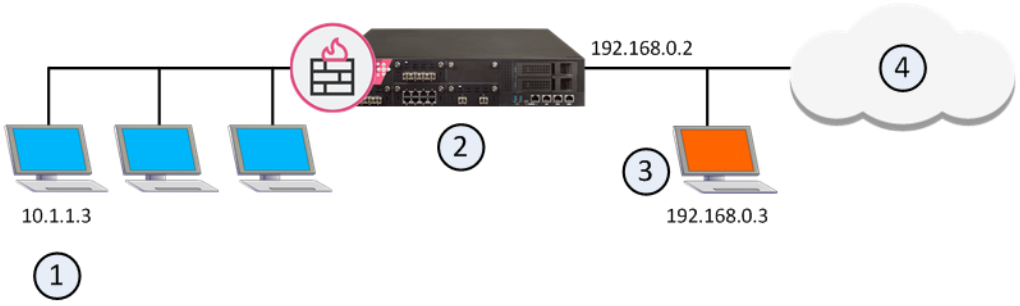
This section includes advanced NAT settings.

Deployment Configurations

This section discusses how to configure NAT in some network deployments.

Automatic and Proxy ARP

Giving a computer on the internal network an IP address from an external network using NAT makes that computer appear on the external network. When NAT on the Security Gateway is configured automatically, the Security Gateway replies on behalf of translated network objects to ARP Requests that are sent from the external network for the IP address of the internal computer.



Item	Description
1	Computer on the internal network with IP address 10.1.1.3
2	Security Gateway with external interface IP address 192.168.0.2 responds to ARP Requests on behalf of translated internal objects
3	Translated IP Address 192.168.0.3 on the external network
4	External network

If you are using manual NAT rules, you must configure Proxy ARP entries to associate the translated IP address with the MAC address of the Security Gateway interface that is on the same network as the translated IP addresses.

See sk30197 http://supportcontent.checkpoint.com/solutions?id=sk30197 for more information about configuring:

- Proxy ARP for IPv4 Manual NAT
- Proxy ARP for Scalable Platforms

See sk91905 http://supportcontent.checkpoint.com/solutions?id=sk91905 for more about configuring Proxy NDP for IPv6 Manual NAT.

NAT and Anti-Spoofing

NAT is performed after Anti-Spoofing checks, which are performed only on the source IP address of the packet. This means that spoofing protection is configured on the interfaces of the Security Gateway in the same way as NAT.

Disabling NAT in a VPN Tunnel

When communicating within a VPN, it is normally not necessary to perform NAT. You can disable NAT in a VPN tunnel with a single click in the VPN community object. Disabling NAT in a VPN tunnel by defining a NAT rule slows down the performance of the VPN.

Connecting Translated Objects on Different Interfaces

The following sections describe how to allow connections in both directions between statically translated objects (hosts, networks or address ranges) on different Security Gateway interfaces.

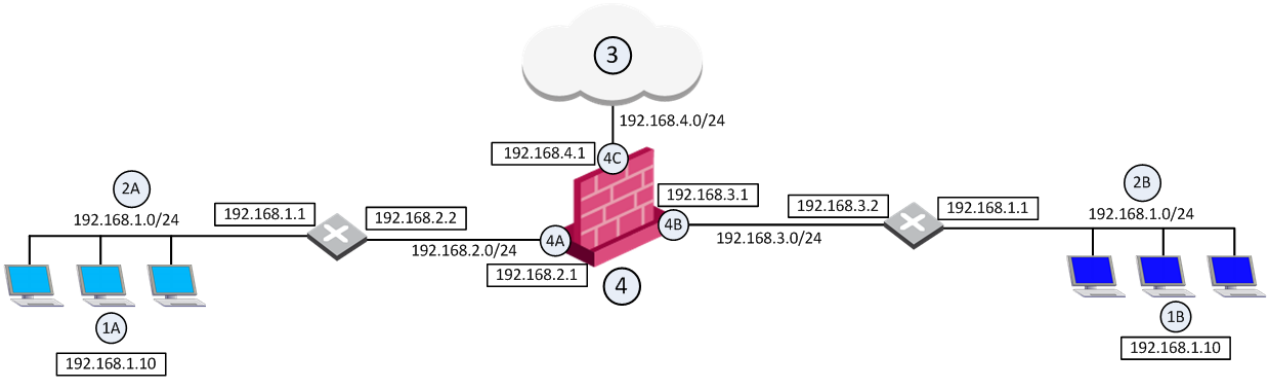
If NAT is defined through the network object (as opposed to using Manual NAT Rules), then you must ensure that bidirectional NAT is enabled.

Internal Communication with Overlapping Addresses

If two internal networks have overlapping (or partially overlapping) IP addresses, Security Gateway enables:

- Communication between the overlapping internal networks.
- Communication between the overlapping internal networks and the outside world.
- Enforcement of a different security policy for each overlapping internal network.

Network Configuration



For example, assume both Network 2A and Network 2B share the same address space (**192.168.1.0/24**), therefore standard NAT cannot be used to enable communication between the two networks. Instead, overlapping NAT must be performed on a per interface basis.

Users in Network 2A who want to communicate with users in Network 2B must use the **192.168.30.0/24** network as a destination. Users in Network 2B who want to communicate with users in Network 2A must use the **192.168.20.0/24** network as a destination.

The Security Gateway (4) translates the IP addresses in the following way for each individual interface:

Interface 4A

- Inbound source IP addresses are translated to the virtual network **192.168.20.0/24**.
- Outbound destination IP addresses are translated to the network **192.168.1.0/24**.

Interface 4B

- Inbound source IP addresses are translated to the network **192.168.30.0/24**.
- Outbound destination IP addresses are translated to the network **192.168.1.0/24**.

Interface 4C

Overlapping NAT is not configured for this interface. Instead, use NAT Hide in the normal way (not on a per-interface basis) to hide source addresses behind the interface's IP address (**192.168.4.1**).

Communication Examples

This section describes how to enable communication between internal networks, and between an internal network and the Internet

Communication Between Internal Networks

If user 1A, at IP address **192.168.1.10** in Network 2A, wants to connect to user 1B, at IP address **192.168.1.10** (the same IP address) in Network 2B, user 1A opens a connection to the IP address **192.168.30.10**.

Communication Between Internal Networks

Step	Source IP address	Destination IP address
Interface 4A — before NAT	**192.168.1.10**	**192.168.30.10**
Interface 4A — after NAT	**192.168.20.10**	**192.168.30.10**
Security Gateway enforces the security policy for packets from network **192.168.20.0/24** to network **192.168.30.0/24**.		
Interface 4B — before NAT	**192.168.20.10**	**192.168.30.10**
Interface 4B — after NAT	**192.168.20.10**	**192.168.1.10**

Communication Between an Internal Network and the Internet

If user 1A, at IP address **192.168.1.10** in network 2A, connects to IP address **192.0.2.10** on the Internet (3).

Communication Between an Internal Network and the Internet

Step	Source IP address	Destination IP address
Interface 4A — before NAT	**192.168.1.10**	**192.0.2.10**
Interface 4A — after NAT	**192.168.20.10**	**192.0.2.10**
The Security Gateway (4) enforces the security policy for packets from network **192.168.20.0/24** to the Internet (3).		
Interface 4C — before NAT	**192.168.20.10**	**192.0.2.10**
Interface 4C — after NAT Hide	**192.168.4.1**	**192.0.2.10**

Routing Considerations

To allow routing from Network 2A to Network 2B, routing must be configured on the Security Gateway.

These sections contain sample routing commands for Windows and Linux operating systems (for other operating systems, use the equivalent commands).

On Windows

- **route add 192.168.30.0 mask 255.255.255.0 192.168.3.2**
- **route add 192.168.20.0 mask 255.255.255.0 192.168.2.2**

On Linux

- **route add -net 192.168.30.0/24 gw 192.168.3.2**
- **route add -net 192.168.20.0/24 gw 192.168.2.2**

Object Database Configuration

To activate the overlapping NAT feature, use GuiDBedit Tool (see sk13009 http://supportcontent.checkpoint.com/solutions?id=sk13009), or dbedit (see skI3301 http://supportcontent.checkpoint.com/solutions?id=skI3301). In the sample network configuration, the per interface values for interface 4A and interface 4B are set in the following wa**y:**

Sample Network Configuration: Interface Configuration

Parameter	Value
enable_overlapping_nat	**true**
overlap_nat_dst_ipaddr	The overlapping IP addresses (before NAT). In the sample network configuration, **192.168.1.0** for both interfaces.
overlap_nat_src_ipaddr	The IP addresses after NAT. In the sample network configuration, **192.168.20.0** for interface 4A, and **192.168.30.0** for interface 4B.
overlap_nat_netmask	The net mask of the overlapping IP addresses. In the sample network configuration, **255.255.255.0**.

Security Management Behind NAT

The Security Management Server sometimes uses a private IP address (as listed in RFC 1918) or some other non-routable IP address, because of the lack of public IP addresses.

NAT (Static or Hide) for the Security Management Server IP address can be configured in one click, while still allowing connectivity with managed gateways. All gateways can be controlled from the Security Management Server, and logs can be sent to the Security Management Server. NAT can also be configured for a Management High Availability server and a Log Server.

Note - Security Management behind NAT is not supported for deployments where the Security Management Server also acts as a gateway and must be addressed from outside the NATed domain, for example, when it receives SAM commands.

In a typical Security Management Behind NAT scenario: the Security Management Server (1) is in a network on which Network Address Translation is performed (the "NATed network"). The Security Management Server can control Security Gateways inside the NATed network, on the border between the NATed network and the outside world and outside the NATed network.

Item	Description
1	Primary_Security_Management object with IP address 10.0.0.1. Translated address 192.168.55.1

In ordinary Hide NAT configurations, connections cannot be established from the external side the NAT A Security Gateway. However, when using Hide NAT on the Security Management Server, gateways can send logs to the Security Management Server.

When using the Security Management behind NAT feature, the remote gateway automatically selects the Security Management address to be addressed and simultaneously applies NAT considerations.

To enable NAT for the Security Management Server:

- From the **NAT** page of the Security Management Server object, define NAT and select **Apply for A Security Gateway control connections**.

Non-Corresponding Gateway Addresses

Sometimes the gateway contacts the Security Management Server with an address that does not correspond to the deployment of the remote gateway. For example:

- When the automatic selection of the gateway does not conform with the routing of the deployment of the gateway . In this case, define the masters and loggers manually, to allow the remote gateway to contact the Security Management Server using the required address. When an inbound connection from a managed gateway enters the Security Gateway, port translation is used to translate the hide address to the real IP address of the Security Management Server.

To define masters and loggers, select **Use local definitions for Log Servers** and **Use local definitions for Masters** and specify the correct IP addresses on the gateway.

This solution encompasses different scenarios:

- The remote gateway addresses the NATed IP when you want it to address the real IP.
- The remote gateway addresses the real IP when you want it to address the NATed IP. In this case, specify the SIC name of the Security Management Server in the masters file.

Notes:

- Only one object can be defined with these settings, unless the second object is defined as a Secondary Security Management Server or as a Domain Log Server.
- Ensure that you properly define the Topology settings on all gateways. All workarounds required for previous versions still function with no changes in their behavior.

Configuring the Security Management Server Object

To configure the Security Management Server object:

1. From the **NAT** page on the Primary_Security_Management object, select either Static NAT or Hide NAT. If using Hide NAT, select **Hide behind IP Address**, for example, **192.168.55.1**. Do not select **Hide behind Gateway** (address **0.0.0.0**).
2. Select **Install on Gateway** to protect the NATed objects or network. Do not select **All**.
3. Select **Apply for Security Gateway control connections**.

Configuring the Security Gateway Object

To configure the Security Gateway object:

1. Open the Security Gateway **Network Management** page
2. Create the Interface. Click **Actions** > **New interface**.
3. In the **General** page of the **Interface** window, define the **IP** address and the Net Mask.

4. In the **Topology** section, click **Modify**.
5. Select **Override**.
6. Select **Network defined by the interface IP and Net Mask**.

IP Pool NAT

An IP Pool is a range of IP addresses (an address range, a network or a group of one of these objects) that is routable to the gateway. IP Pool NAT ensures proper routing for encrypted connections for the following two connection scenarios:

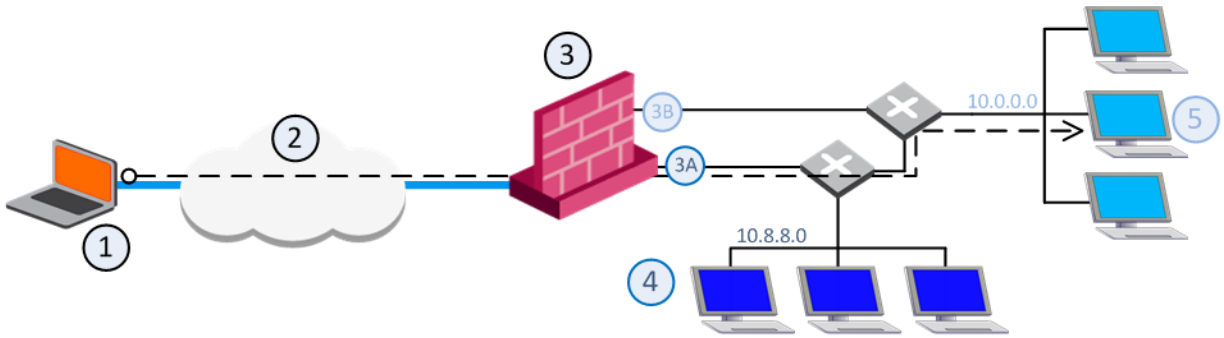
- Remote Access Client to MEP (Multiple Entry Point) gateways
- Gateway to MEP gateways

When a connection is opened from a Remote Access Client or a client behind a gateway, to a server behind the MEP Gateways, the packets are routed through one of the MEP gateways. Return packets in the connection must be routed back through the same gateway in order to maintain the connection. To ensure that this occurs, each of the MEP gateways maintains a pool of IP addresses that are routable to the gateway. When a connection is opened to a server, the gateway substitutes an IP address from the IP pool for the source IP address. Reply packets from the server return to the gateway, which restores the original source IP address and forwards the packets to the source.

IP Pool Per Interface

You can define a separate IP address pool on one or more of the gateway interfaces instead of defining a single pool of IPs for the gateway.

Defining an IP pool per interface solves routing issues that occur when the gateway has more than two interfaces. Sometimes it is necessary that reply packets return to the gateway through the same gateway interface. This illustration shows one of the MEP Gateways in a Remote Access Client to MEP (Multiple Entry Point) gateway deployment.



Item	Description
1	Packets from source host: Source: Original Destination:
2	VPN tunnel through the Internet
3	MEP Gateway

Item	Description
3A	IP Pool 1 packets: Source: 10.55.8.x Destination:
3B	IP Pool 2 packets: Source: 10.55.10.x Destination:
4	Internal network 10.8.8.0
5	Target host in internal network 10.10.10.0

If a remote client opens a connection to the internal network, reply packets from hosts inside the internal networks are routed to the correct gateway interface through the use of static IP pool NAT addresses.

The remote client's IP address is NATed to an address in the IP pool on one of the gateway interfaces. The addresses in the IP pool can be routed only through that gateway interface so that all reply packets from the target host are returned only to that interface. Therefore, it is important that the IP NAT pools of the interfaces do not overlap.

When the packet returns to the gateway interface, the gateway restores the remote peer's source IP address.

The routing tables on the routers that lie behind the gateway must be edited so that addresses from a gateway IP pool are returned to the correct gateway interface.

Switching between IP Pool NAT per gateway and IP Pool NAT per interface and then installing the security policy deletes all IP Pool allocation and all NATed connections.

NAT Priorities

IP Pool NAT can be used both for encrypted (VPN) and non-encrypted (decrypted by the gateway) connections.

Note - To enable IP Pool NAT for clear connections through the gateway, configure INSPECT changes in the **user.def** file (see sk98239 http://supportcontent.checkpoint.com/solutions?id=sk98239). Contact Check Point Technical Support.

For non-encrypted connections, IP Pool NAT has the following advantages over Hide NAT:

- New back connections (for example, X11) can be opened to the NATed host.
- User-to-IP server mapping of protocols that allow one connection per IP can work with a number of hosts instead of only one host.
- IPsec, GRE and IGMP protocols can be NATed using IP Pool NAT (and Static NAT). Hide NAT works only with TCP, UDP and ICMP protocols.

Because of these advantages, you can specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.

The order of NAT priorities are:

1. Static NAT
2. IP Pool NAT

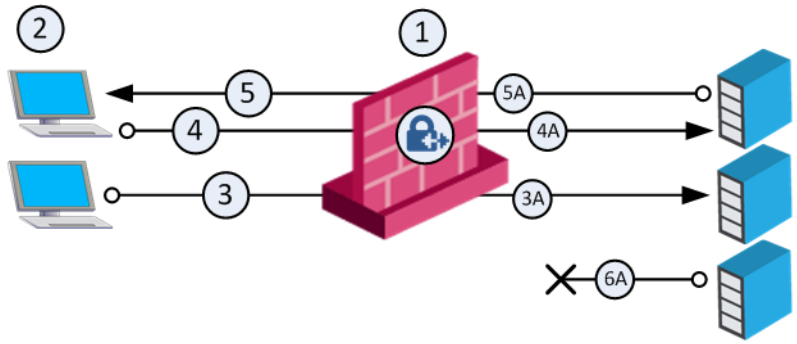
3. Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

Reusing IP Pool Addresses For Different Destinations

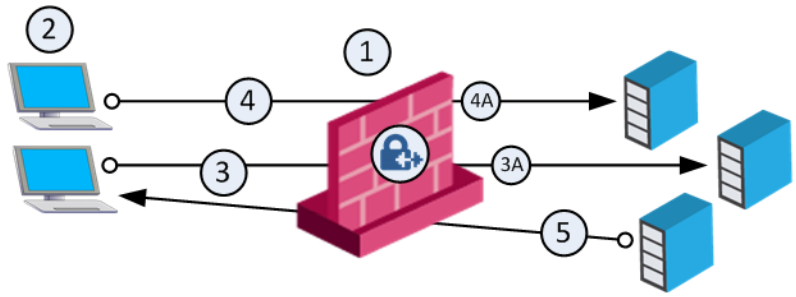
IP Pool addresses can be reused for different destinations, which makes more efficient use of the addresses in the pool. If a pool contains N addresses, then any number of clients can be assigned an IP from the pool as long as there are no more than N clients per server.

Using IP Pool allocation per destination, two different clients can receive the same IP from the pool as long as they communicate with different servers (connections 1 and 2). When reusing addresses from the IP Pool, back connections are supported from the original server only (connection 3). This means that connections back to the client can be opened only from the specific server to which the connection was opened.



Item	Description
1	Gateway with IP Pool addresses A to Z
2	Clients. Source: Original Destination:
3A	NATed packet from connection 3. Source: A Destination:
4A	NATed packet from connection 4. Source: A Destination:
5A	NATed packet from reply connection 5. Source: Original Destination: A
6A	This server cannot open a connection with Destination A back to the client.

The default **Do not reuse IP Pool NAT** behavior means that each IP address in the IP Pool is used once (connections 1 and 2 in the following illustration). In this mode, if an IP pool contains 20 addresses, up to 20 different clients can be NATed and back connections can be opened from any source to the client (connection 3).



Item	Description
1	Gateway with IP Pool addresses A to Z.
2	Clients. Source: Original Destination:
3A	NATed packet from connection 3. Source: A Destination:
4A	NATed packet from connection 4. Source: Z Destination:
5	Connection. Source: Original Destination: A

Switching between the **Reuse** and **Do not reuse** modes and then installing the security policy, deletes all IP Pool allocations and all NATed connections.

Configuring IP Pool NAT

To configure IP Pool NAT:

1. From the SmartConsole **Menu**, select **Global Properties**.
2. In the **Global Properties** > **NAT** page, select **Enable IP Pool NAT** and the required tracking options.
3. In the gateway **General Properties** page, ensure the gateway version is specified correctly.
4. For each gateway or gateway interface, create a network object that represents its IP pool NAT addresses. The IP pool can be a network, group, or address range. For example, for an address range, do the following:

   a) From the **Objects Bar (F11)**, In the network objects tree, select **New > More > Network Object > Address Range > Address Range**.

   The **Address Range Properties** window opens.

b) In the **General** tab, enter the first and last IP of the address range.

c) Click **OK**. The new address range appears in the **Address Ranges** branch of the network objects tree.

5. Edit the gateway object, and select **NAT** > **IP Pool NAT**.
6. In the **IP Pool NAT** page, select one of the following:

   a) **Allocate IP Addresses from** and then select the address range you created to configure IP Pool NAT for the whole gateway, or

   b) **Define IP Pool NAT on Gateway interfaces** to configure IP Pool NAT per interface.
7. If required, select one or more of the following options:

   a) **Use IP Pool NAT for VPN client connections**

   b) **Use IP Pool NAT for gateway to gateway connections**

   c) **Prefer IP Pool NAT over Hide NAT** to specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.
8. Click **Advanced**.

   a) **Return unused addresses to IP Pool after**: Addresses in the pool are reserved for 60 minutes (default), even if the user logs off. If the user disconnects from their ISP and then redials and reconnects, there will be two Pool NAT addresses in use for the user until the first address from the IP Pool times out. If users regularly lose their ISP connections, you may want to decrease the time-out to prevent the IP Pool from being depleted.

   b) **Reuse IP addresses from the pool for different destinations**: This is a good option unless you need to allow back connections to be opened to clients from any source, rather than just from the specific server to which the client originally opened the connection.
9. Click **OK**.
10. Edit the routing table of each internal router so that packets with an IP address assigned from the NAT pool are routed to the appropriate gateway or, if using IP Pools per interface, the appropriate gateway interface.

IP Pool NAT for Clusters

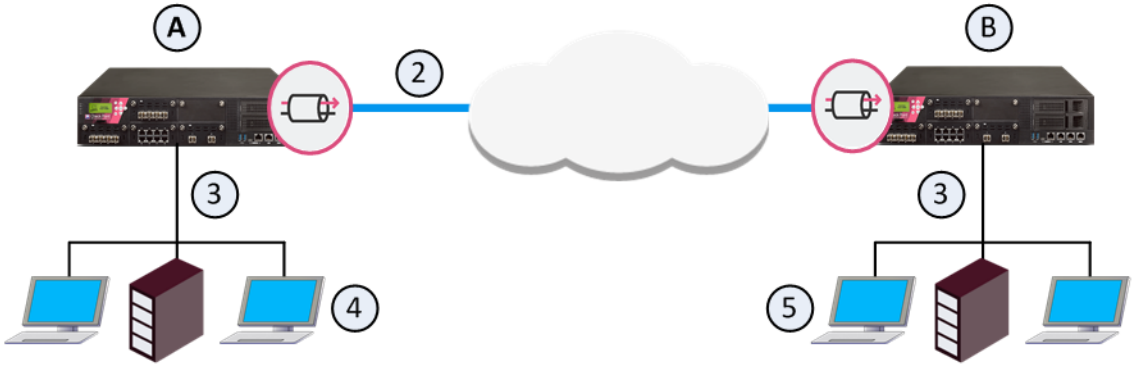
IP Pools for gateway clusters are configured in two places in SmartConsole:

- In the gateway Cluster object **NAT > IP Pool NAT** page, select the connection scenario.
- In the Cluster member object **IP Pool NAT** page, define the IP Pool on the cluster member. A separate IP pool must be configured for each cluster member. It is not possible to define a separate IP Pool for each cluster member interface.

Site-to-Site VPN

The basis of Site-to-Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.

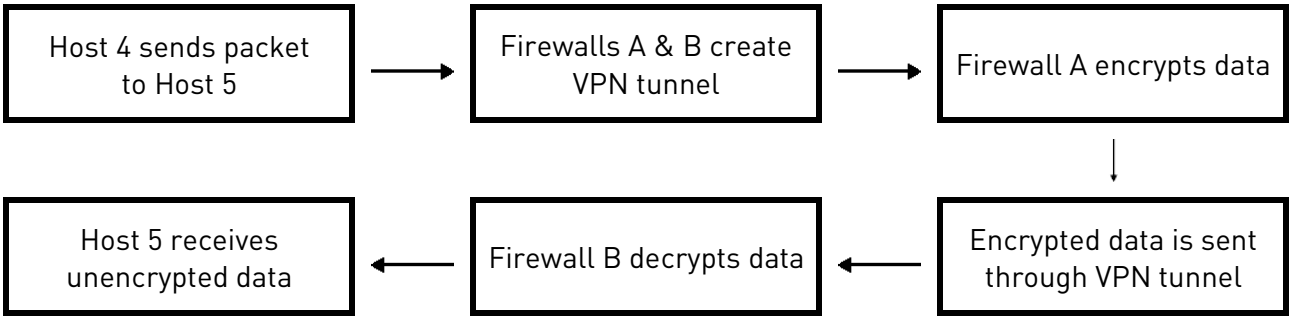
Sample Site-to-Site VPN Deployment



Item	Description
A, B	Security Gateways
2	VPN tunnel
3	Internal network in VPN domain
4	Host 4
5	Host 5

In this sample VPN deployment, Host 4 and Host 5 securely send data to each other. The Security Gateways do IKE negotiation and create a VPN tunnel. They use the IPsec protocol to encrypt and decrypt data that is sent between Host 4 and Host 5.

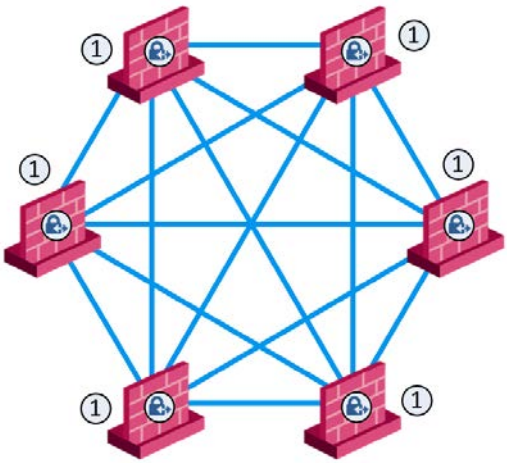
VPN Workflow



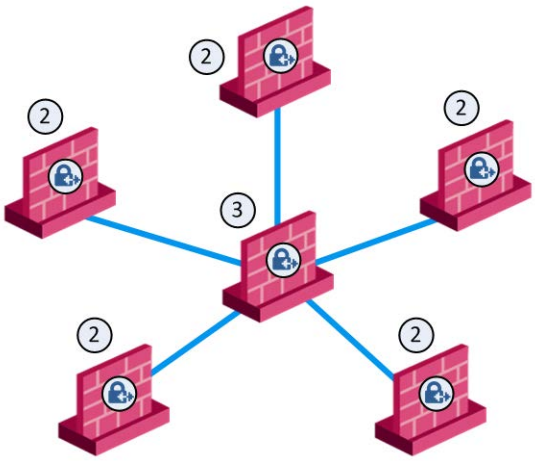
VPN Communities

A VPN Domain is a collection of internal networks that use Security Gateways to send and receive VPN traffic. Define the resources that are included in the VPN Domain for each Security Gateway. Then join the Security Gateways into a VPN community - collection of VPN tunnels and their attributes. Network resources of different VPN Domains can securely communicate with each other through VPN tunnels that terminate at the Security Gateways in the VPN communities.

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN tunnels between each pair of Security Gateway. In a Star community, each satellite Security Gateway has a VPN tunnel to the central Security Gateway, but not to other Security Gateways in the community.



Mesh Topology



Star Topology

Item	Description
1	Security Gateway
2	Satellite Security Gateways
3	Central Security Gateway

Sample Star Deployment

This section explains how to configure a VPN star community. This deployment lets the satellite Security Gateways connect to the internal network of the central Security Gateway. The internal network object is named: **Internal-network**.

To create a new VPN Star Community:

1. In SmartConsole, go to the **Security Policies** page.
2. In the **Access Tools** section, click **VPN Communities**.
3. Click **New** and select **Star Community**.
   The **New Star Community** window opens.
4. Enter the name for the community.
5. From the navigation tree, select **Encryption**.
6. Configure the VPN encryption methods and algorithms for the VPN community.
7. Click **OK**.

To configure star VPN for the Security Gateways:

For each Security Gateway in the VPN community, follow these configuration steps.

1. In SmartConsole, go to the **Gateways & Servers** page and double-click the Security Gateway object.
   The gateway properties window opens.
2. In the **Network Security** section of the **General Properties** page, select **IPsec VPN**.
3. From the navigation tree, go to **Network Management > VPN Domain**.

- For the central Security Gateway, click **Manually defined** and select the **Internal-network** object
- For a satellite Security Gateway, select **All IP addresses**

4. From the navigation tree, click **IPsec VPN**.
5. Configure the Security Gateway as a member of a VPN star community.
   a) In the **This Security Gateway participates in the following VPN Communities** section, click **Add**.

      The **Add this Gateway to Community** window opens.

   b) Select the VPN Community and click **OK**.
6. Click **OK**.

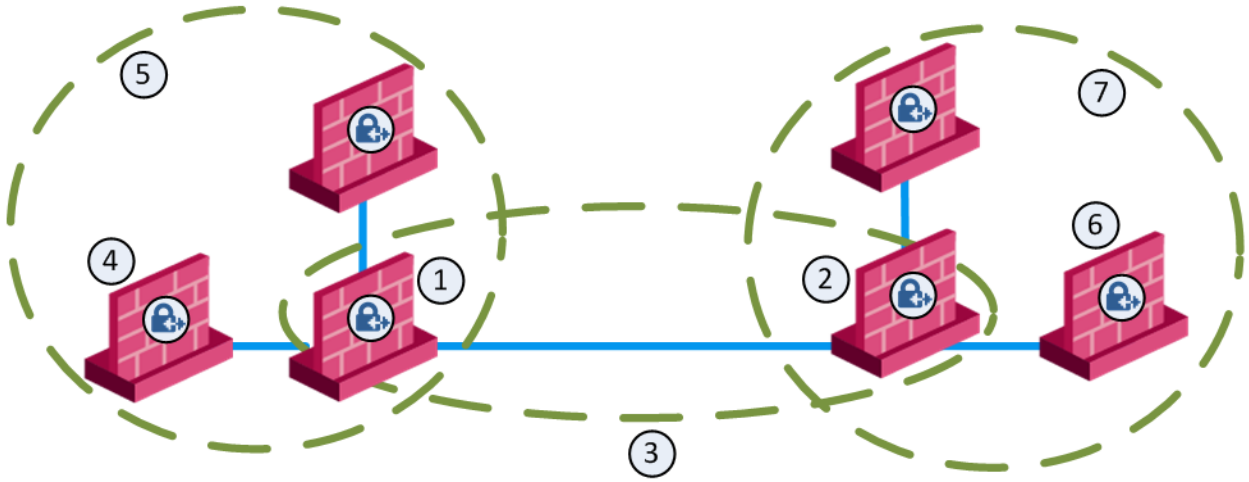
After you create a community and configure Security Gateways, add those Security Gateways to the community as a center or as a satellite gateway.

To add a Security Gateway to a new star community:

1. In SmartConsole, go to the **Security Policies** page.
2. In the **Access Tools** section, click **VPN Communities**.
3. Select the new star community and click **Edit**.

   The **Star Community** window opens.
4. In the **Gateways** page, add Security Gateways to the community:
   - **Center Gateways** - Click **Add** and select center gateways. Select **Mesh center gateways**, if necessary.
   - **Satellite Gateways** - Click **Add** and select satellite gateways.
5. Click **OK**.

Sample Combination VPN Community



Item	Description
1	London Security Gateway
2	New York Security Gateway
3	London - New York Mesh community

Item	Description
4	London company partner (external network)
5	London Star community
6	New York company partner (external network)
7	New York Star community

This deployment is composed of a Mesh community for London and New York Security Gateways that share internal networks. The Security Gateways for external networks of company partners do not have access to the London and New York internal networks. However, the Star VPN communities let the company partners access the internal networks of the sites that they work with.

Allowing VPN Connections

To allow VPN connections between Security Gateways in specific VPN communities, add Access Control rules that accept such connections.

To allow all VPN traffic to hosts and clients on the internal networks of a specific VPN community, select these options in the **Encrypted Traffic** section of the properties configuration window for that VPN Community:

- For a meshed community: **Accept all encrypted traffic**
- For a Star Community: **Accept all encrypted traffic on Both center and satellite gateways**, or **Accept all encrypted traffic on Satellite gateways only**.

Sample VPN Access Control Rules

This table shows sample VPN rules for an Access Control Rule Base. (The **Action**, **Track** and **Time** columns are not shown. **Action** is set to **Allow**, **Track** is set to **Log**, and **Time** is set to **Any**.)

No.	Name	Source	Destination	VPN	Service	Install On
1	-	Any	**NEGATED** Member Gateways	BranchOffices LondonOffices	Any	BranchOffices LondonOffices
2	Site-to-site VPN	Any	Any	All_GwToGw	FTP-port HTTP HTTPS SMTP	Policy Targets
3	Remote access	Any	Any	RemoteAccess	HTTP HTTPS IMAP	Policy Targets

1. Automatic rule that SmartConsole adds to the top of the *Implied Rules* when the **Accept All Encrypted Traffic** configuration option is selected for the `BranchOffices` VPN community and the `LondonOffices` VPN community. This rule is installed on all the Security Gateways in these communities. It allows all VPN traffic to hosts and clients on the internal networks of

these communities. Traffic that is sent to the Security Gateways in these VPN communities is dropped.

Note - This automatic rule can apply to more than one VPN community.

2. **Site-to-site VPN** - Connections between hosts in the VPN Domains of all Site-to-Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.
3. **Remote access** - Connections between hosts in the VPN Domains of Remote Access VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

To Learn More About Site-to-Site VPN

To learn more about site-to-Site VPN, see the *R80.10 Site-to-Site VPN Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=53104.

Remote Access VPN

If employees remotely access sensitive information from different locations and devices, system administrators must make sure that this access does not become a security vulnerability. Check Point's Remote Access VPN solutions let you create a VPN tunnel between a remote user and the internal network. The Mobile Access Software Blade extends the functionality of Remote Access solutions to include many clients and deployments.

VPN Connectivity Modes

When securely connecting remote clients with the internal resources, organizations face connectivity challenges, such as these:

- The IP addresses of a remote access client might be unknown
- The remote access client can be connected to a LAN with internal IP addresses (such as, at hotels)
- It is necessary for the remote client to use protocols that are not supported

The Check Point IPsec VPN Software Blade provides these VPN connectivity modes to help organizations resolve those challenges:

- **Office Mode**

  Remote users can be assigned the same or non-routable IP addresses from the local ISP. Office Mode solves these routing problems and encapsulates the IP packets with an available IP address from the internal network. Remote users can send traffic as if they are in the office and avoid VPN routing problems.

- **Visitor Mode**

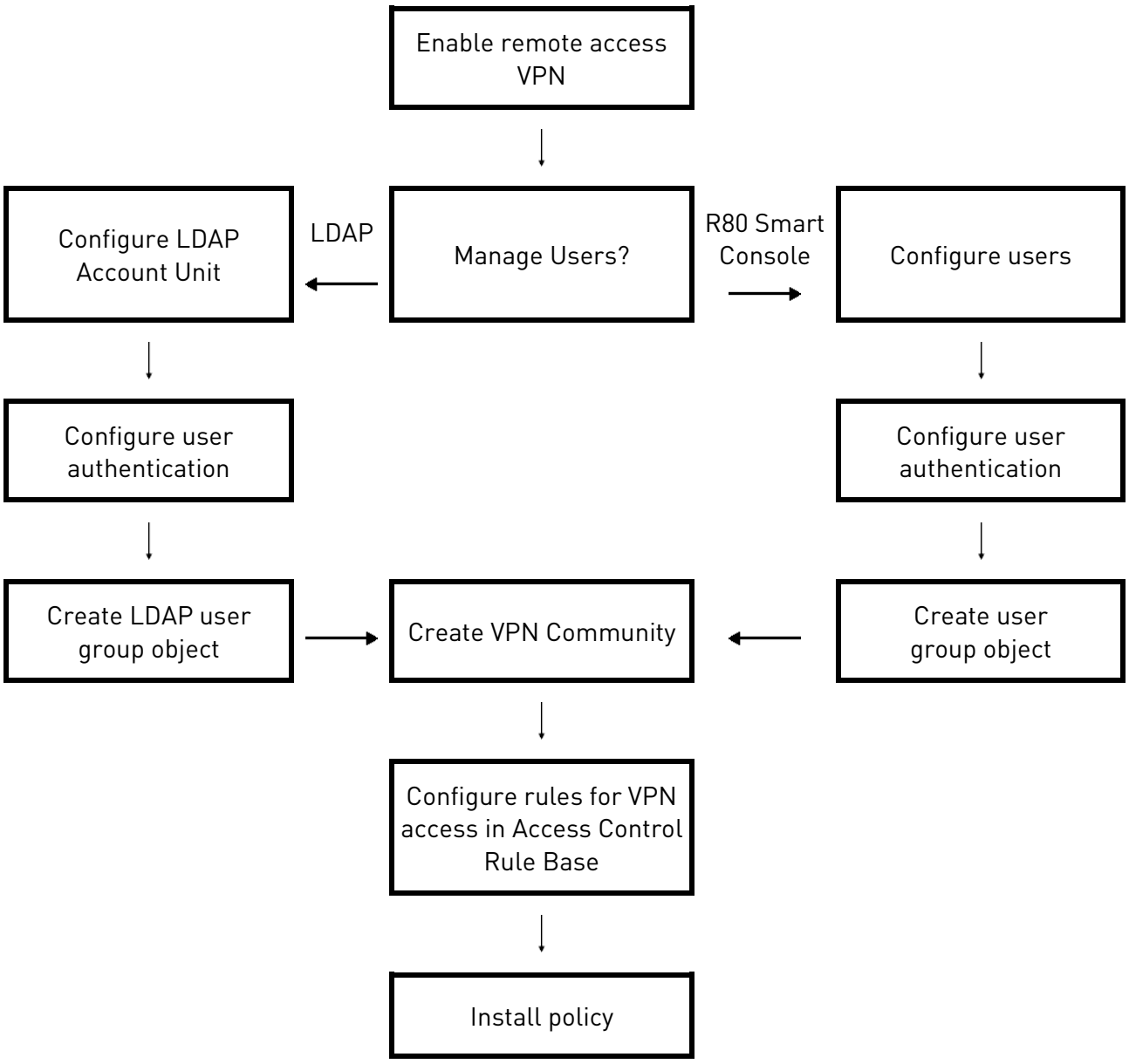
  Remote users can be restricted to using only HTTP and HTTPS protocols. Visitor Mode lets these users tunnel all protocols through regular TCP connections on port 443.

Sample Remote Access VPN Workflow

Here is an example of a Remote Access VPN workflow:

1. Use SmartConsole to enable Remote Access VPN on the Security Gateway.
2. Add the remote user information to the Security Management Server:
   - Create and configure an LDAP Account Unit
   - Enter the information in the SmartConsole user database

   Optional - Configure the gateway for remote user authentication (optional).
3. Define the gateway Access Control and encryption rules.
4. Create the group objects to use in the gateway rules:
   - **LDAP Group** object - for an LDAP Account Unit
   - **User Group** object - for users configured in the SmartConsole user database
5. Create and configure the encryption settings for the VPN community object in **Global Properties** > **Remote Access** > **VPN - Authentication and Encryption**.
6. Add Access Control rules to the Access Control Rule Base to allow VPN traffic to the internal networks.



Configuring the Security Gateway for a Remote Access Community

Make sure that the VPN Software Blade is enabled before you configure the Remote Access community.

To configure the Security Gateway for Remote Access:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **IPsec VPN**.
   The page shows the VPN communities that the Security Gateway is participating.
3. To add the Security Gateway to a Remote Access community:
   a) Click **Add**.
   b) Select the community.
   c) Click **OK**.
4. From the navigation tree, click **Network Management > VPN Domain**.
5. Configure the VPN Domain.
6. Configure the settings for Visitor Mode.
7. From the navigation tree, click **VPN Clients > Office Mode**.
8. Configure the settings for Office Mode.
   Note - Office Mode support is mandatory on the Security Gateway side.
9. Click **OK** and publish the changes.

To Learn More About Remote Access VPN

To learn more about Remote Access VPN, see the R*80.10 Remote Access VPN Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=53105.

Mobile Access to the Network

Check Point Mobile Access lets remote users easily and securely use the Internet to connect to internal networks. Remote users start a standard HTTPS request to the Mobile Access Security Gateway, and authenticate with one or more secure authentication methods.

The Mobile Access Portal lets mobile and remote workers connect easily and securely to critical resources over the internet. Check Point Mobile Apps enable secure encrypted communication from unmanaged smartphones and tablets to your corporate resources. Access can include internal apps, email, calendar, and contacts.

To include access to Mobile Access applications in the Rule Base, include the **Mobile Application** in the **Services & Applications** column.

To give access to resources through specified remote access clients, create Access Roles for the clients and include them in the **Source** column of a rule.

Check Point Mobile Access Solutions

Check Point Mobile Access has a range of flexible clients and features that let users access internal resources from remote locations. All these solutions include these features:

- Enterprise-grade, secure connectivity to corporate resources
- Strong user authentication
- Granular access control

For more information about the newest versions of Mobile Access solutions and clients, go to sk67820 http://supportcontent.checkpoint.com/solutions?id=sk67820.

Client-Based vs. Clientless

Check Point remote access solutions use IPsec and SSL encryption protocols to create secure connections. All Check Point clients can work through NAT devices, hotspots, and proxies in situations with complex topologies, such as airports or hotels. These are the types of installations for remote access solutions:

- **Client-based** - Client application installed on endpoint computers and devices. The client supplies access to most types of corporate resources according to the access privileges of the user.
- **Clientless** - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.
- **On demand client** - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

Mobile Access Clients

- Capsule Workspace - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
- Capsule Connect - A full L3 tunnel app that gives users network access to all mobile applications.
- Check Point Mobile for Windows - A Windows IPsec VPN client that supplies secure IPsec VPN connectivity and authentication.

Mobile Access Web Portal

The Mobile Access Portal is a clientless SSL VPN solution that supplies secure access to web-based resources. After users authenticate to the portal, they can access Mobile Access applications such as Outlook Web App and a corporate wiki.

SSL Network Extender

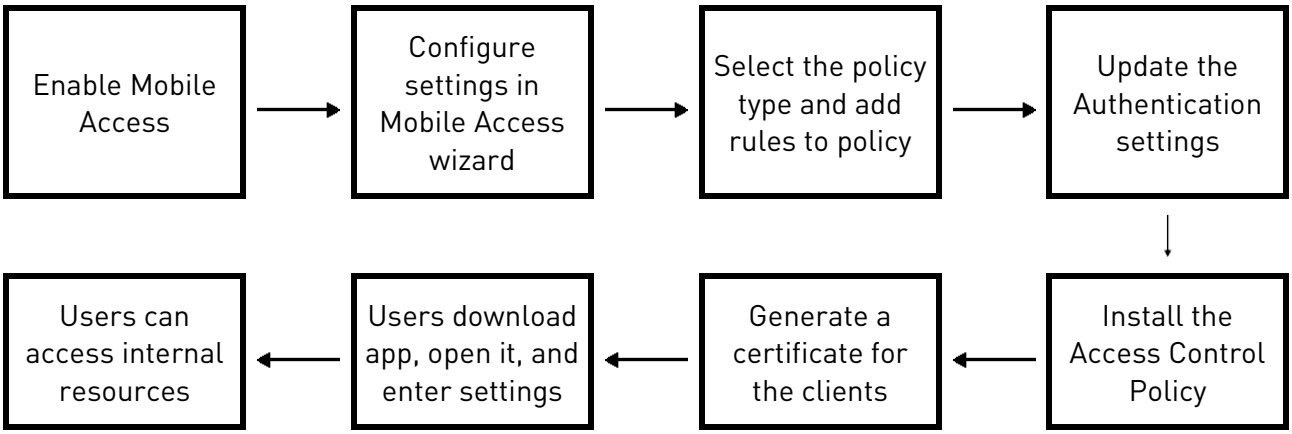
SSL Network Extender is an on-demand SSL VPN client and is installed on the computer or mobile device from an Internet browser. It supplies secure access to internal network resources.

Configuring Mobile Access to Network Resources

Sample Mobile Access Workflow

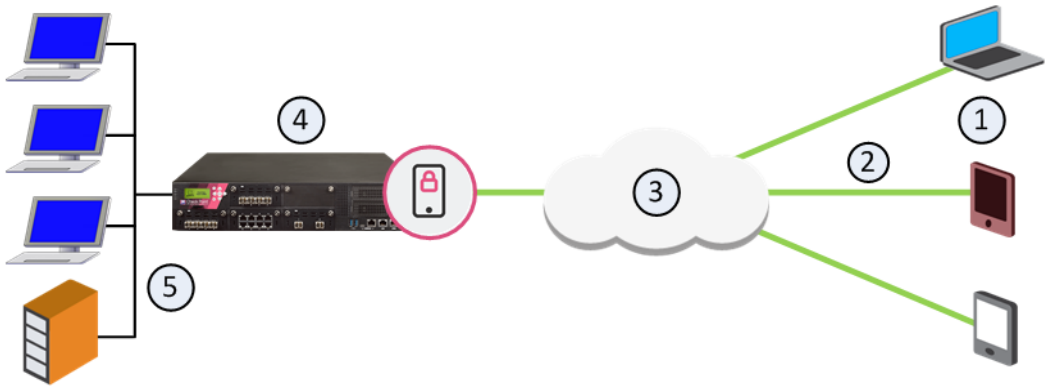
This is a high-level workflow to configure remote access to Mobile Access applications and resources.

1. Use SmartConsole to enable the Mobile Access Software Blade on the gateway.
2. Follow the steps in the Mobile Access Configuration wizard to configure these settings:
   a) Select mobile clients.
   b) Define the Mobile Access portal.
   c) Define applications, for example Outlook Web App.
   d) Connect to the AD server for user information.
3. Select the policy type:
   - The default is to use the Legacy Policy, configured in the **Mobile Access** tab in SmartConsole.
   - To include Mobile Access in the **Unified Access Control Policy**, select this in **Gateway Properties** > **Mobile Access**.
4. Add rules to the Policy:
   - For Legacy Policy: Add rules in SmartConsole. Select **Security Policies** > **Shared Policies** > **Mobile Access** > **Open Mobile Access Policy in SmartConsole**
   - For Unified Access Control Policy: Add rules in SmartConsole > **Security Policies Access Control Policy**.
5. Configure the authentication settings in **Gateway Properties** > **Mobile Access** > **Authentication**.
6. Install the Access Control Policy on the gateway.
   Users can access mobile applications through the configured Mobile Access portal with the defined authentication method.
7. Optional: Give secure access to users through the Capsule Workspace app with certificate authentication.
   a) In the gateway **Mobile Access** > **Authentication,** click **Settings**, and select **Require client certificate**.
   b) Use the Certificate Creation and Distribution Wizard (in the **Security Policies** view > **Client Certificates** > **New**.
   c) Users download the Capsule Workspace app.
   d) Users open the Capsule Workspace app and enter the Mobile Access Site Name and necessary authentication, such as user name and password.



Sample Mobile Access Deployment

This is a sample deployment of a Mobile Access Security Gateway with an AD and Exchange server in the internal network.



Item	Description
1	Mobile devices
2	Mobile Access tunnels
3	Internet (external networks)
4	Mobile Access Security Gateway
5	Internal network resources, AD and Exchange servers

In this sample Mobile Access deployment, a mobile device uses a Mobile Access tunnel to connect to the internal network. The Mobile Access Security Gateway decrypts the packets and authenticates the user. The connection is allowed and the mobile device connects to the internal network resources.

Using the Mobile Access Configuration Wizard

This procedure describes how to enable and configure the Mobile Access Software Blade on a Security Gateway with the Configuration wizard. For this sample configuration, the AD user group **Mobile_Access** contains all the users that are allowed to connect to the internal network. The deployment is based on the Sample Mobile Access Deployment (on page 169).

This configuration lets these clients connect to internal resources:

- Android and iOS mobile devices
- Windows and Mac computers
- Internet browsers can open a SSL Network Extender connection to the internal network

To configure Mobile Access:

1. In SmartConsole, go to **Gateways & Servers** and double-click the gateway object.
   The **General Properties** window opens.
2. In the **General Properties** > **Network Security** section, select **Mobile Access**.
   The **Mobile Access** page of the **Mobile Access Configuration Wizard** opens.
3. Configure the Security Gateway to allow connections from the Internet and mobile devices.
   Select these options:
   - **Web**
   - **Mobile Devices** - Select the required options.
   - **Desktops/Laptops -** Select the required options.
4. Click **Next**.
   The **Web Portal** page opens.
5. Enter the primary URL for the Mobile Access portal. The default is
   `https://<gw_IPv4>/sslvpn`
6. Click **Next**.
   The **Applications** page opens.
7. Configure the applications to show:
   a) In **Web Applications**, make sure **Demo web application (World Clock)** is selected.
   b) In **Mail/Calendar/Contacts**, enter the domain for the Exchange server and select:
      - **Mobile Mail (including push mail notifications)**
      - **ActiveSync Applications**
      - **Outlook Web App**

      The Mobile Access portal shows links to the Demo web and Outlook Web App applications.
      The client on the mobile device shows links to the other applications.
8. Click **Next**.
   The **Active Directory** page opens.
9. Select the AD domain and enter the user name and password.
10. Click **Connect**.
    The Security Gateway makes sure that it can connect to the AD server.
11. Click **Next**.
    The **Users** page opens.
    Click **Add** and then select the group **Mobile_Access**.
12. Click **Next** and then click **Finish**.
    The **Mobile Access Configuration Wizard** closes.
13. Click **OK**.
    The **Gateway Properties** window closes.

Allowing Mobile Connections

The Mobile Access Configuration Wizard enables and configures the Mobile Access Software Blade. It is necessary to add Firewall rules to allow connections from the VPN clients on the computers and devices. Create a Host Node object for the Exchange server, all of the other objects are predefined.

Name	Source	Destination	VPN	Service	Action	Install On	Track
Mobile Access Users	Any	ExchngSrvr	RemoteAccess	HTTP HTTPS MSExchange	Accept	MobileAccessGW	Log

All connections from the `RemoteAccess` VPN community to the Exchange server are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and MS Exchange. This rule is installed on Security Gateways in the `MobileAccessGW` group.

Defining Access to Applications

Use the **Security Policies** page in SmartConsole to define rules that let users access Mobile Access applications. The applications that are selected in the Configuration Wizard are automatically added to this page. You can also create and edit the rules that include these SmartConsole objects:

- Users and user groups
- Mobile Access applications
- Mobile Access Security Gateways

Activating Single Sign On

Enable the SSO (Single Sign On) feature to let users authenticate one time for applications that they use during Mobile Access sessions. The credentials that users enter to log in to the Mobile Access portal can be re-used automatically to authenticate to different Mobile Access applications. SSO user credentials are securely stored on the Mobile Access Security Gateway for that session and are used again if users log in from different remote devices. After the session is completed, the credentials are stored in a database file.

By default, SSO is enabled on new Mobile Access applications that use HTTP. Most Web applications authenticate users with specified Web forms. You can configure SSO for an application to use the authentication credentials from the Mobile Access portal. It is not necessary for users to log in again to each application.

To configure SSO:

1. In SmartConsole, go to **Security Policies > Shared Policies > Mobile Access**.
2. Click **Open Mobile Access Policy in SmartDashboard**.
3. In the **Mobile Access** tab, select **Additional Settings** > **Single Sign On**.
   The **Single Sign On** page opens.
4. Select an application and click **Edit**.
   The application properties window opens and shows the **Single Sign On** page.
5. For Web form applications:
   a) In the **Application Single Sign On Method** section, select **Advanced** and click **Edit**.

The **Advanced** window opens.

b) Select **This application reuses the portal credentials. Users are not prompted**.

c) Click **OK**.

d) Select **This application uses a Web form to accept credentials from users**.

e) Click **OK**.

6. Install the policy.

Connecting to a Citrix Server

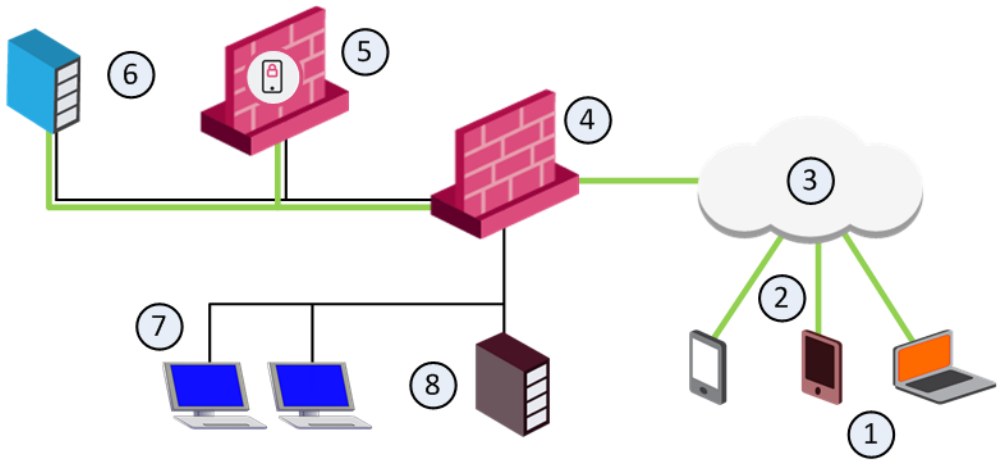
Citrix Services

The Mobile Access Software Blade integrates the Firewall Citrix clients and services. It is not necessary to use STA (Secure Ticketing Authority) servers in a Mobile Access Security Gateway deployment because Mobile Access uses its own STA engine. You can also use Mobile Access in a deployment with STA and CSG (Citrix Secure Gateway) servers.

The Mobile Access server certificate must use a FQDN (Fully Qualified Domain Name) that is issued to the FQDN of the Mobile Access Security Gateway.

Sample Deployment with Citrix Server

This is a sample deployment of a Mobile Access Security Gateway and a Citrix web server in the DMZ. The Citrix XenApp server is connected to the internal network.



Item	Description
1	Mobile devices
2	Mobile Access tunnels
3	Internet (external networks)
4	Security Gateway for the internal network
5	Mobile Access Security Gateway in the DMZ
6	Citrix web interface
7	Internal network resources
8	Citrix XenApp (MetaFrame) server

Configuring Citrix Services for Mobile Access

This procedure describes how to configure Mobile Access to let remote users connect to Citrix applications. The deployment is based on the Sample Deployment with Citrix Server (on page 173).

To configure Citrix services:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the Mobile Access, click **Configure in SmartDashboard**.
3. In the **Mobile Access** tab, click **Applications** > **Citrix Services**.
4. Click **New**.
   The **General Properties** page of the **Citrix Service** window opens.
5. Enter the **Name** for the Citrix server object.
6. From the navigation tree, click **Web Interface**.
7. Create a new object for the Citrix web interface server, in **Servers**, click **Manage** > **New** > **Host**.
   The **Host Node** window opens.
8. Enter the settings for the Citrix web interface server and the click **OK**.
9. In Services, select one or more of these services that the Citrix web interface server supports:
   - HTTP
   - HTTPS
10. From the navigation tree, click **Link in Portal**.
11. Configure the settings for the link to the Citrix services in the Mobile Access portal:
    - **Link text** - The text that is shown for the Citrix link
    - **URL** - The URL for the directory or subdirectory of the Citrix application
    - **Tooltip** - Text that is shown when the user pauses the mouse pointer above the Citrix link
12. From the navigation tree, select **Additional Settings** > **Single Sign On**.
13. Enable Single Sign On for Citrix services, select these options:
    - **Turn on single Sign On for this application**
    - **Prompt users for their credentials, and store them for future use**
14. Click **OK**.
    The Citrix server object is added to **Defined Citrix Services**.
15. From the Mobile Access navigation tree, select **Policy**.
16. Add the Citrix services object to the applicable rules.
    a) Right-click on the Applications cell of a rule and select **Add Applications**.
    b) Select the Citrix services object.
17. Install the policy.

Compliance Check

The Mobile Access Software Blade lets you use the Endpoint Security on Demand feature to create compliance policies and add more security to the network. Mobile devices and computers are scanned one time to make sure that they are compliant before they can connect to the network.

The compliance scanner is installed on mobile devices and computers with ActiveX (for Internet Explorer on Windows) or Java. The scan starts when the Internet browser tries to open the Mobile Access Portal.

Compliance Policy Rules

The compliance policy is composed of different types of rules. You can configure the security and compliance settings for each rule or use the default settings.

These are the rules for a compliance policy:

- Windows security - Microsoft Windows hotfixes, patches and Service Packs.
- Anti-Spyware protection - Anti-Spyware software.
- Anti-Virus protection - Anti-Virus software version and virus signature files.
- Firewall - Personal firewall software.
- Spyware scan - Action that is done for different types of spyware.
- Custom - Compliance rules for your organization, for example: applications, files, and registry keys.
- OR group - A group of the above rules. An endpoint computer is compliant if it meets one of the rules in the group.

Creating a Compliance Policy

By default, Endpoint Security on Demand only allows endpoint computers that are compliant with the compliance policy log in to the Mobile Access portal.

To create a compliance policy:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the Mobile Access section, click **Configure in SmartDashboard**.
3. In the **Mobile Access** tab, select **Endpoint Security on Demand** > **Endpoint Compliance**.
4. Click **Edit policies**.
   The **Policies** window opens.
5. Click **New Policy**.
   The **Policies** > **New Policy** window opens.
6. Enter the **Name** and **Description** for the policy.
7. Click **Add**.
   The **Add Enforcement Rules** window opens.
8. Select rules for the policy.
   You can also create new rules - click **New Rule**, and configure the rule settings.
9. Click **OK**.
   The **Policies** > **New Policy** window shows the rules for the policy.

10. Select **Bypass spyware scan** if necessary.

    When selected, the scan for endpoint computers that are compliant with the Anti-Virus or Anti-Spyware settings is changed. These computers do not scan for spyware when they connect to a Mobile Access Security Gateway.
11. Click **OK**.

    The **Policies** window opens.
12. Click **OK**.

Configuring Compliance Settings for a Security Gateway

The Firewall on a Mobile Access Security Gateway only allows access to endpoint computers that are compliant with the compliance policy.

This procedure shows how to configure the Laptop Computer policy ("Compliance Policy Rules" on page 175) for a Security Gateway.

To configure the compliance settings:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the **Mobile Access** section, click **Configure in SmartDashboard**.
3. In the **Mobile Access** tab, select **Endpoint Security on Demand > Endpoint Compliance**.
4. Select the Security Gateway and click **Edit**.

   The **Endpoint Compliance** page of the Security Gateway properties window opens.
5. Select **Scan endpoint machine when user connects**.
6. Select **Threshold policy** and from the drop-down menu select **Laptop Computer**.
7. Click **OK**.
8. Install the policy on the Mobile Access Security Gateway.

Secure Workspace

Secure Workspace is a security solution that allows remote users to connect to enterprise network resources safely and securely. The Secure Workspace virtual workspace provides a secure environment on endpoint computers that is segregated from the "real" workspace. Users can only send data from this secure environment through the Mobile Access portal. Secure Workspace users can only access permitted applications, files, and other resources from the virtual workspace.

Secure Workspace creates an encrypted folder on the computer called **My Secured Documents** and can be accessed from the virtual desktop. This folder contains temporary user files. When the session terminates, Secure Workspace deletes this folder and all other session data.

For more about configuring Secure Workspace, see the *R80.10 Mobile Access Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=53103.

To enable Secure Workspace on a Mobile Access Security Gateway:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the **Mobile Access** section, click **Configure in SmartDashboard**.

   Legacy SmartDashboard opens.
3. In the **Mobile Access** tab, click **Endpoint Security on Demand** > **Secure Workspace**.
4. Select the Security Gateway and click **Edit**.

The **Check Point Secure Workspace** page of the Security Gateway properties window opens.

5. Select **This gateway supports access to applications from within Check Point Secure Workspace**.
6. Click **OK** and then install the policy.

To Learn More About Mobile Access

To learn more about Mobile Access VPN, see the *R80.10 Mobile Access Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=53103.

Creating a Threat Prevention Policy

In This Section:

Threat Prevention Components

To challenge today's malware landscape, Check Point's comprehensive Threat Prevention solution offers a multi-layered, pre- and post-infection defense approach and a consolidated platform that enables enterprise security to detect and block modern malware. These Threat Prevention Software Blades are available:

- IPS - A complete IPS cyber security solution, for comprehensive protection against malicious and unwanted network traffic, which focuses on application and server vulnerabilities, as well as in-the-wild attacks by exploit kits and malicious attackers.
- Anti-Bot - Post-infection detection of bots on hosts. Prevents bot damages by blocking bot C&C (Command and Control) communications. The Anti-Bot Software Blade is continuously updated from ThreatCloud, a collaborative network to fight cybercrime. Anti-Bot discovers infections by correlating multiple detection methods.
- Anti-Virus - Pre-infection detection and blocking of malware at the gateway. The Anti-Virus Software Blade is continuously updated from ThreatCloud. It detects and blocks malware by correlating multiple detection engines before users are affected.
- SandBlast:
  - Threat Emulation - Protection against infections from undiscovered exploits, zero-day and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network. The ThreatCloud Emulation service reports to the ThreatCloud and automatically shares the newly identified threat information with other Check Point customers.
  - Threat Extraction - Protection against incoming malicious content. To remove possible threats, the Threat Extraction blade creates a safe copy of the file, while the Threat Emulation Software Blade inspects the original file for potential threats.

Each Software Blade gives unique network protections. When combined, they supply a strong Threat Prevention solution. Data from malicious attacks are shared between the Threat Prevention Software Blades and help to keep your network safe. For example, the signatures from threats that Threat Emulation identifies are added to the ThreatCloud for use by the other Threat Prevention blades.

IPS

The IPS Software Blade delivers complete and proactive intrusion prevention. It delivers 1,000s of signatures, behavioral and preemptive protections. It gives another layer of security on top of Check Point firewall technology. IPS protects both clients and servers, and lets you control the network usage of certain applications. The hybrid IPS detection engine provides multiple defense layers which allows it excellent detection and prevention capabilities of known threats, and in many cases future attacks as well. It also allows unparalleled deployment and configuration flexibility and excellent performance.

Elements of Protection

IPS protection include:

- Detection and prevention of specific known exploits.
- Detection and prevention of vulnerabilities, including both known and unknown exploit tools, for example protection from specific CVEs.
- Detection and prevention of protocol misuse which in many cases indicates malicious activity or potential threat. Examples of commonly manipulated protocols are HTTP, SMTP, POP, and IMAP.
- Detection and prevention of outbound malware communications.
- Detection and prevention of tunneling attempts. These attempts may indicate data leakage or attempts to circumvent other security measures such as web filtering.
- Detection, prevention or restriction of certain applications which, in many cases, are bandwidth consuming or may cause security threats to the network, such as Peer to Peer and Instant Messaging applications.
- Detection and prevention of generic attack types without any pre-defined signatures, such as Malicious Code Protector.

Check Point constantly updates the library of protections to stay ahead of emerging threats.

Capabilities of IPS

The unique capabilities of the Check Point IPS engine include:

- Clear, simple management interface.
- Reduced management overhead by using one management console for all Check Point products
- Integrated management with SmartConsole.
- Easy navigation from business-level overview to a packet capture for a single attack.
- #1 security coverage for Microsoft and Adobe vulnerabilities.
- Resource throttling so that high IPS activity will not impact other blade functionality
- Complete integration with Check Point configuration and monitoring tools in SmartConsole, to let you take immediate action based on IPS information.

For example, some malware can be downloaded by a user unknowingly when he browses to a legitimate web site, also known as a drive-by-download. This malware can exploit a browser vulnerability to create a special HTTP response and sending it to the client. IPS can identify and block this type of attack even though the firewall may be configured to allow the HTTP traffic to pass.

Anti-Bot

A bot is malicious software that can infect your computer. It is possible to infect a computer when you open attachments that exploit a vulnerability, or go to a web site that results in a malicious download.

When a bot infects a computer, it:

- Takes control of the computer and neutralizes its Anti-Virus defenses. It is not easy to find bots on your computer, they hide and change how they look to Anti-Virus software.
- Connects to a C&C (Command and Control center) for instructions from cyber criminals. The cyber criminals, or bot herders, can remotely control it and instruct it to do illegal activities without your knowledge. Your computer can do one or more of these activities:
  - Steal data (personal, financial, intellectual property, organizational)
  - Send spam
  - Attack resources (Denial of Service Attacks)
  - Consume network bandwidth and reduce productivity

One bot can often create multiple threats. Bots are frequently used as part of **Advanced Persistent Threats** (APTs) where cyber criminals try to damage individuals or organizations.

The Anti-Bot Software Blade detects and prevents these bot and botnet threats. A botnet is a collection of compromised and infected computers.

The Anti-Bot Software Blade uses these procedures to identify bot infected computers:

- **Identify the C&C addresses used by criminals to control bots**

  These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

- **Identify the communication patterns used by each botnet family**

  These communication fingerprints are different for each family and can be used to identify a botnet family. Research is done for each botnet family to identify the unique language that it uses. There are thousands of existing different botnet families and new ones are constantly emerging.

- **Identify bot behavior**

  Identify specified actions for a bot such as, when the computer sends spam or participates in DoS attacks.

After the discovery of bot infected machines, the Anti-Bot Software Blade blocks outbound communication to C&C sites based on the Rule Base. This neutralizes the threat and makes sure that no sensitive information is sent out.

Identifying Bot Infected Computers

The Anti-Bot Software Blade uses these procedures to identify bot infected computers:

- **Identify the C&C addresses used by criminals to control bots**

  These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

- **Identify the communication patterns used by each botnet family**

These communication fingerprints are different for each family and can be used to identify a botnet family. Research is done for each botnet family to identify the unique language that it uses. There are thousands of existing different botnet families and new ones are constantly emerging.

- **Identify bot behavior**

  Identify specified actions for a bot such as, when the computer sends spam or participates in DoS attacks.

Preventing Bot Damage

After the discovery of bot infected machines, the Anti-Bot Software Blade blocks outbound communication to C&C sites based on the Rule Base. This neutralizes the threat and makes sure that no sensitive information is sent out.

ThreatSpect Engine and ThreatCloud Repository

The ThreatSpect engine is a unique multi-tiered engine that analyzes network traffic and correlates information across multiple layers to find bots and other malware. It combines information on remote operators, unique botnet traffic patterns and behavior to identify thousands of different botnet families and outbreak types.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

The Security Gateway gets automatic binary signature and reputation updates from the ThreatCloud repository. It can query the cloud for new, unclassified IP/URL/DNS resources that it finds.

The layers of the ThreatSpect engine:

- **Reputation** - Analyzes the reputation of URLs, IP addresses and external domains that computers in the organization access. The engine searches for known or suspicious activity, such as a C&C.
- **Signatures** - Detects threats by identifying unique patterns in files or in the network.
- **Suspicious Mail Outbreaks** - Detects infected machines in the organization based on analysis of outgoing mail traffic.
- **Behavioral Patterns** - Detects unique patterns that indicate the presence of a bot. For example, how a C&C communicates with a bot-infected machine.

Anti-Virus

Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats (combinations of malicious code and vulnerabilities for infection and dissemination) and trojans.

The Anti-Virus Software Blade scans incoming and outgoing files to detect and prevent these threats. It also gives pre-infection protection from malware contained in these files.

The Anti-Virus Software Blade:

- Identifies malware in the organization using the ThreatSpect engine and ThreatCloud repository:
  - Prevents malware infections from incoming malicious files types (Word, Excel, PowerPoint, PDF, etc.) in real-time. Incoming files are classified on the gateway and the result is then sent to the ThreatCloud repository for comparison against known malicious files, with almost no impact on performance.
  - Prevents malware download from the internet by preventing access to sites that are known to be connected to malware. Accessed URLs are checked by the gateway caching mechanisms or sent to the ThreatCloud repository to determine if they are permissible or not. If not, the attempt is stopped before any damage can take place.
- Uses the ThreatCloud repository to receive binary signature updates and query the repository for URL reputation and Anti-Virus classification.

SandBlast

Cyber-threats continue to multiply and now it is easier than ever for criminals to create new malware that can easily bypass existing protections. On a daily basis, these criminals can change the malware signature and make it virtually impossible for signature-based products to protect networks against infection. To get ahead, enterprises need a multi-faceted prevention strategy that combines proactive protection that eliminates threats before they reach users. With Check Point's Threat Emulation and Threat Extraction technologies, SandBlast provides zero-day protection against unknown threats that cannot be identified by signature-based technologies.

Threat Emulation

Threat Emulation gives networks the necessary protection against unknown threats in files that are attached to emails. The Threat Emulation engine picks up malware at the exploit phase, before it enters the network. It quickly quarantines and runs the files in a virtual sandbox, which imitates a standard operating system, to discover malicious behavior before hackers can apply evasion techniques to bypass the sandbox.

When emulation is done on a file:

- The file is opened on more than one virtual computer with different operating system environments.
- The virtual computers are closely monitored for unusual and malicious behavior, such as an attempt to change registry keys or run an unauthorized process.
- Any malicious behavior is immediately logged and you can use Prevent mode to block the file from the internal network.
- The cryptographic hash of a new malicious file is saved to a database and the internal network is protected from that malware.
- After the threat is caught, a signature is created for the new (previously unknown) malware which turns it into a known and documented malware. The new attack information is automatically shared with Check Point ThreatCloud to block future occurrences of similar threats at the gateway.

If the file is found not to be malicious, you can download the file after the emulation is complete.

Learn more about Threat Emulation.

Threat Extraction

Threat Extraction is supported on R77.30 and higher.

The Threat Extraction blade extracts potentially malicious content from e-mail attachments before they enter the corporate network. To remove possible threats, the Threat Extraction does one of these two actions:

- Creates a safe copy of the file, or
- Extracts exploitable content out of the file.

Threat Extraction delivers the reconstructed file to users and blocks access to the original suspicious version, while Threat Emulation analyzes the file in the background. This way, users have immediate access to content, and can be confident they are protected from the most advanced malware and zero-day threats.

Threat Emulation runs in parallel to Threat Extraction for version R80.10 and higher.

Here are examples for exploitable content in Microsoft Office Suite Applications and PDF files:

- Queries to databases where the query contains a password in the clear
- Embedded objects
- Macros and JavaScript code that can be exploited to propagate viruses
- Hyperlinks to sensitive information
- Custom properties with sensitive information
- Automatic saves that keep archives of deleted data
- Sensitive document statistics such as owner, creation and modification dates
- Summary properties
- PDF documents with:
  - Actions such as launch, sound, or movie URIs
  - JavaScript actions that run code in the reader's Java interpreter
  - Submit actions that transmit the values of selected fields in a form to a specified URL
  - Incremental updates that keep earlier versions of the document
  - Document statistics that show creation and modification dates and changes to hyperlinks
  - Summarized lists of properties

Before you enable the Threat Extraction blade, you must deploy the gateway as a Mail Transfer Agent.

Assigning Administrators for Threat Prevention

You can control the administrator Threat Prevention permissions with a customized Permission Profile. The customized profile can have different Read/Write permissions for Threat Prevention policy, settings, profiles and protections.

Analyzing Threats

Networks today are more exposed to cyber-threats than ever. This creates a challenge for organizations in understanding the security threats and assessing damage.

SmartConsole helps the security administrator find the cause of cyber-threats, and remediate the network.

The **Logs & Monitor** > **Logs** view presents the threats as logs.

The other views in the **Logs & Monitor** view combine logs into meaningful security events. For example, malicious activity that occurred on a host in the network, in a selected time interval (the last hour, day, week or month). They also show pre- and post-infections statistics.

You can create rich and customizable views and reports for log and event monitoring, which inform key stakeholders about security activities. For each log or event, you can see a lot of useful information from the Threat Wiki and IPS Advisories about the malware, the virus or the attack.

Out-of-the-Box Protection from Threats

In This Section:

Getting Quickly Up and Running with the Threat Prevention Policy

You can configure Threat Prevention to give the exact level of protection that you need, but you can also configure it to provide protection right out of the box.

To get quickly up and running with Threat Prevention:

1. Enable the Threat Prevention blades on the gateway.
2. **Install Policy**.

After you enable the blades and install the policy, this rule is generated:

Name	Protected Scope	Action	Track	Install On
Out-of-the-box Threat Prevention policy	Any	Optimized	Log Packet Capture	Policy Targets

Notes:

- The **Optimized** ("Optimized Protection Profile Settings" on page 189) profile is installed by default.
- The **Protection/Site** column is used only for protection exceptions.

Enabling the Threat Prevention Software Blades

Enabling the IPS Software Blade

Enable the IPS Software Blade on the Security Gateway.

To enable the IPS Software Blade:

1. In the **Gateways & Servers** view, double-click the gateway object.
   The **General Properties** window opens.
2. In the **General Properties** > **Network Security** tab, click **IPS**.
3. Follow the steps in the wizard that opens.
4. Click **OK**.
5. Click **OK** in the **General Properties** window.
6. **Install Policy** ("Installing the Threat Prevention Policy" on page 188).

Enabling the Anti-Bot Software Blade

To enable the Anti-Bot Software Blade on a Security Gateway:

1. In the **Gateways & Servers** view, double-click the gateway object.
   The **General Properties** window of the gateway opens.
2. From the **Network Security** tab, select **Anti-Bot**.
   The **Anti-Bot and Anti-Virus First Time Activation** window opens.
3. Select an activation mode option:
   - **According to the Anti-Bot and Anti-Virus policy** - Enable the Anti-Bot Software Blade and use the Anti-Bot settings of the Threat Prevention profile in the Threat Prevention policy.
   - **Detect only** - Packets are allowed, but the traffic is logged according to the settings in the Threat Prevention Rule Base.
4. Click **OK**.
5. **Install Policy** ("Installing the Threat Prevention Policy" on page 188).

Enabling the Anti-Virus Software Blade

Enable the Anti-Virus Software Blade on a Security Gateway.

To enable the Anti-Virus Software Blade:

1. In the **Gateways & Servers** view, double-click the gateway object.
   The **General Properties** window of the gateway opens.
2. From the **Network Security** tab, click **Anti-Bot**.
   The **Anti-Bot and Anti-Virus First Time Activation** window opens.
3. Select one of the activation mode options:
   - **According to the Anti-Bot and Anti-Virus policy** - Enable the Anti-Virus Software Blade and use the Anti-Virus settings of the Threat Prevention profile in the Threat Prevention policy.
   - **Detect only** - Packets are allowed, but the traffic is logged according to the settings in the Threat Prevention Rule Base.
4. Click **OK**
5. **Install Policy** ("Installing the Threat Prevention Policy" on page 188).

Enabling SandBlast Threat Emulation Software Blade

Use the First Time Configuration Wizard in SmartConsole to enable Threat Emulation in the network. Configure the Security Gateway or Emulation appliance for your deployment.

Using Cloud Emulation

Files are sent to the Check Point ThreatCloud over a secure SSL connection for emulation. The emulation in the ThreatCloud is identical to emulation in the internal network, but it uses only a small amount of CPU, RAM, and disk space of the Security Gateway. The ThreatCloud is always up-to-date with all available operating system environments.

Best Practice - For ThreatCloud emulation, it is necessary that the Security Gateway connects to the Internet. Make sure that the DNS and proxy settings are configured correctly in **Global Properties**.

To enable ThreatCloud emulation:

1. In the **Gateways & Servers** view, double-click the Security Gateway object.
   The **Gateway Properties** window opens.
2. From the **Network Security** tab, select **SandBlast Threat Emulation**.
   The **Threat Emulation First Time Configuration Wizard** opens and shows the **Emulation Location** page.
3. Select **ThreatCloud Emulation Service**.
4. Click **Next**.
   The **Summary** page opens.
5. Click **Finish** to enable Threat Emulation and close the First Time Configuration Wizard.
6. Click **OK**.
   The **Gateway Properties** window closes.
7. **Install Policy** ("Installing the Threat Prevention Policy" on page 188).

Sample Workflow - Creating a Threat Emulation Profile

This is a sample workflow to create a Threat Prevention profile that includes Threat Emulation.

To create a Threat Prevention profile for Threat Emulation:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Click **New**.
4. Enter the **Name** for the Threat Prevention profile.
5. In **Blades Activation**, select the Threat Prevention Software Blades.
6. Configure the **Activation Mode** settings for the traffic.
7. From the **Threat Emulation Settings** page, set the **Prevent** and **Ask** UserCheck settings.
8. From the navigation tree, click **Threat Emulation > General**.
9. Configure the Threat Emulation **Protected Scope** for this profile, and define how traffic from external and internal networks are sent for emulation.
10. Select one or more **Protocols** for this profile.
    The Software Blade runs emulation only for files and traffic that match the selected protocols.
11. Configure the **File Types** for this profile.
    The Software Blade runs emulation only for files that match the selected file types.
12. Click **OK** and **install Policy**.

Enabling the SandBlast Threat Extraction Blade

To enable the Threat Extraction Blade:

1. In the Gateways & Servers view, right-click the gateway object and select **Edit**.
   The **Gateway Properties** window opens.
2. On the **General Properties** > **Network Security** tab, select **SandBlast Threat Extraction**.
   The **Threat Extraction First Time Activation Wizard** opens.
3. Enable the gateway as a **Mail Transfer Agent** (MTA).
   From the drop-down box, select a mail server for forwarded emails.

4. Click **Next**.
5. Click **Finish**.

   Note: In a ClusterXL HA environment, do this once for the cluster object.

Configuring LDAP

If you use LDAP for user authentication, you must activate User Directory for Security Gateways.

To activate User Directory:

1. Open **SmartConsole** > **Global Properties**.
2. On the **User Directory** page, select **Use User Directory for Security Gateways**.
3. Click **OK**.

Installing the Threat Prevention Policy

The IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction Software Blades have a dedicated Threat Prevention policy. You can install this policy separately from the policy installation of the Access Control Software Blades. Install only the Threat Prevention policy to minimize the performance impact on the Security Gateways.

To install the Threat Prevention policy:

1. From the Global toolbar, click **Install Policy**.

   The **Install Policy** window opens showing the installation targets (Security Gateways).
2. Select **Threat Prevention**.
3. Select **Install Mode:**
   - **Install on each selected gateway independently** - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways.

     If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.
4. Click **OK**.

Introducing Profiles

Check Point Threat Prevention provides instant protection based on pre-defined Threat Prevention **Profiles**. You can also configure a custom Threat Prevention profile to give the exact level of protection that the organization needs.

When you install a Threat Prevention policy on the Security Gateways, they immediately begin to enforce IPS protection on network traffic.

A Threat Prevention profile determines which protections are activated, and which Software Blades are enabled for the specified rule or policy. The protections that the profile activates depend on the:

- Performance impact of the protection.

- Severity of the threat.
- Confidence that a protection can correctly identify an attack.
- Settings that are specific to the Software Blade.

A Threat Prevention profile applies to one or more of the Threat Prevention Software Blades: IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction.

A *profile* is a set of configurations based on:

- *Activation settings* (prevent, detect, or inactive) for each *confidence level* of protections that the ThreatSpect engine analyzes
- IPS Settings
- Anti-Bot Settings
- Anti-Virus Settings
- Threat Emulation Settings
- Threat Extraction Settings
- Indicator configuration
- Malware DNS Trap configuration
- Links inside mail configuration

Without profiles, it would be necessary to configure separate rules for different activation settings and confidence levels. With profiles, you get customization and efficiency.

SmartConsole includes these default Threat Prevention profiles:

- **Optimized** - Provides excellent protection for common network products and protocols against recent or popular attacks
- **Strict** - Provides a wide coverage for all products and protocols, with impact on network performance
- **Basic** - Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance

Optimized Protection Profile Settings

The **Optimized** profile is activated by default, because it gives excellent security with good gateway performance.

These are the goals of the Optimized profile, and the settings that achieve those goals:

Goal	Parameter	Setting
Apply settings to all the Threat Prevention Software Blades	**Blades Activation**	Activate the profile for IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction.
Do not have a critical effect on performance	**Performance impact**	Activate protections that have a *Medium or lower* effect on performance.
Protect against important threats	**Severity**	Protect against threats with a severity of *Medium or above*.

Goal	Parameter	Setting
Reduce false-positives	**Confidence**	Set to *Prevent* the protections with an attack *confidence* of *Medium* or *High*. Set to *Detect* the protections with a confidence of *Low*.

Predefined Rule

When you enable one of the Threat Prevention Software Blades, a predefined rule is added to the Rule Base. The rule defines that all traffic for all network objects, regardless of who opened the connection, (the protected scope value equals any) is inspected for all protections according to the optimized profile. By default, logs are generated and the rule is installed on all Security Gateways that use a Threat Prevention Software Blade.

The result of this rule (according to the Optimized profile) is that:

- All protections that can identify an attack with a high or medium confidence level, have a medium or lower performance impact, and a medium or above severity are set to **Prevent** mode.
- All protections that can identify an attack with a low confidence level, have a medium or lower performance impact, and a medium or above severity, are set to **Detect** mode.

Use the **Logs & Monitor** page to show logs related to Threat Prevention traffic. Use the data there to better understand the use of these Software Blades in your environment and create an effective Rule Base. You can also directly update the Rule Base from this page.

You can add more exceptions that prevent or detect specified protections or have different tracking settings.

The Threat Prevention Policy

In This Section:

Workflow for Creating a Threat Prevention Policy

Threat Prevention lets you customize profiles that meet the needs of your organization.

Ideally, you might want to set all protections to Prevent in order to protect against all potential threats. However, to let your gateway processes focus on handling the most important traffic and report only the most concerning threats, you need to determine the most effective way to apply the Threat Prevention settings.

When you define a new Threat Prevention profile, you can create a Threat Prevention Policy which activates only the protections that you need and prevents only the attacks that most threaten your network.

This is the high-level workflow to create and deploy a Threat Prevention policy:

1. Enable the Threat Prevention Software Blades on the Security Gateways.
2. Update the IPS database and Malware database with the latest protections.
3. Optional: Create Policy Packages.
4. Optional: For each Policy Package, create Threat Prevention Policy Layers.

   Note - For each Policy Layer, configure a Threat Prevention Rule Base with the Threat Prevention profile as the *Action* of the rule.
5. Install the Threat Prevention policy.

Threat Prevention Policy Layers

You can create a Threat Prevention Rule Base with multiple Ordered Layers. Ordered Layers help you organize your Rule Base to best suit your organizational needs. You can divide the Ordered Layers by Software Blades, services or networks. Each Ordered Layer calculates its action separately from the other Layers. If a connection matches a rule in only one Layer, then the action enforced is the action in that rule. When a connection matches rules in more than one Layer, the gateway enforces the strictest action and settings.

Important - When Threat Emulation and Threat Extraction run in MTA mode, the gateway enforces the action of the first rule matched. It does not necessarily enforce the strictest rule.

Action Enforcement in Multiple-Layered Security Policies

These examples show which action the gateway enforces when a connection matches rules in more than one Ordered Layers.

Example 1

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect

Enforced action: Prevent

Example 2

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect
Exception for protection X	Inactive	-

Enforced action for protection X: Detect

Example 3

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect
Override for protection X	Detect	-
Exception for protection X	Inactive	-

Exception is prior to override and profile action. Therefore, the action for the Data Center Layer is Inactive.

The action for the Corporate LAN Layer is Detect.

Enforced action for protection X: Detect.

Example 4

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Deep Scan all files	Process specific file type families: Inspect doc files and Drop rtf files.

Enforced action: Deep Scan doc files and Drop rtf files.

Example 5

MIME nesting level and Maximum archive scanning time

The strictest action is:

Block combined with the minimum nesting level/scanning time, or

Allow combined with the maximum nesting level/scanning time, or

If both Block and Allow are matched, the enforced action is Block.

Example 6

UserCheck

	HR Layer	Finance Layer	Data Center Layer 3
Rule matched	Rule 3	Rule 1	Rule 4
Profile action	Detect	Prevent	Prevent
Configured page	Page A	Page B	Page C

The first Layer with the strictest action is enforced.

Enforced Action: Prevent with UserCheck Page B.

Creating a New Ordered Layer

This section explains how to create a new Threat Prevention Ordered Layer. You can configure reuse of Threat Prevention Ordered Layers in different Policy Packages, and set different administrator permissions per Threat Prevention Layer.

To create a new Threat Prevention Layer:

1. In SmartConsole, go to **Menu** > **Manage policies and layers** > **Layers** > **Threat Prevention**.
2. Click **New**.

   The New Threat Prevention Layer window opens.
3. Enter the Layer Name.
4. Optional: In the **General** tab, in the **Sharing** area, you can configure reuse of the layer in different policy packages. Select **Multiple policies and rules can use this layer**.
5. In the **Permissions** tab, select the permission profiles that can edit this layer.

   Note - There is no need to add permission profiles that are configured to edit all layers.
6. **Install Policy**.

Threat Prevention Layers in Pre-R80 Gateways

In pre-R80 versions, the IPS Software Blade was not part of the Threat Prevention Policy, and was managed separately. In R80.xx versions, the IPS Software Blade is integrated into the Threat Prevention Policy.

When you upgrade SmartConsole to R80.xx from earlier versions, with some gateways upgraded to R80.xx, and other gateways remaining in previous versions:

- For pre-R80 gateways with IPS and Threat Prevention Software Blades enabled, the policy is split into two parallel layers: IPS and Threat Prevention.

  To see which gateway enforces which IPS profile, look at the **Install On** column in the IPS Layer.
- R80.xx gateways are managed separately, based on the R80 or higher Ordered Layers ("Threat Prevention Policy Layers" on page 191).

Best Practice - For better performance, we recommend that you use the Optimized profile when you upgrade to R80 or higher from earlier versions.

Threat Prevention Rule Base

Each Threat Prevention Layer contains a Rule Base. The Rule Base determines how the system inspects connections for malware.

The Threat Prevention rules use the Malware database and network objects. Security Gateways that have Identity Awareness enabled can also use Access Role objects as the **Protected Scope** in a rule. The Access Role objects let you easily make rules for individuals or different groups of users.

There are no implied rules in this Rule Base, traffic is allowed or not allowed based on how you configure the Rule Base. For example, A rule that is set to the **Prevent** action, blocks activity and communication for that malware.

Creating Threat Prevention Rules

In This Section:

Create and manage the policy for the Threat Prevention Software Blade as part of the Threat Prevention Policy.

- The **Threat Prevention** page shows the rules and exceptions for the Threat Prevention policy. The rules set the Threat profiles for the network objects or locations defined as a protected scope.

Click the **Add Rule** button to get started.

- You can configure the Threat Prevention settings in the Threat Prevention profile for the specified rule.
- To learn about bots and protections, look through the Threat Wiki.

Best Practice - Disable a rule when you work on it. Enable the rule when you want to use it. Disabled rules do not affect the performance of the Gateway. To disable a rule, right click in the **No.** column of the rule and select **Disable.**

Configuring IPS Profile Settings

To configure IPS settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **IPS** > **Additional Activation**.
5. Configure the customized protections for the profile.
6. From the navigation tree, click **IPS** > **Updates**.
7. Configure the settings for newly downloaded IPS protections ("Updates" on page 196).
8. If you import IPS profiles from a pre-R80 deployment:
   a) From the navigation tree, click **IPS** > **Pre-R80 Settings**.
   b) Activate the applicable **Client** and **Server** protections.
   c) Configure the IPS protection categories to exclude from this profile.

   Note - These categories are different from the protections in the **Additional Activation** page.
9. Click **OK**.
10. **Install Policy**.

Updates

There are numerous protections available in IPS. It takes time to become familiar with those that are relevant to your environment. Some are easily configured for basic security and can be safely activated automatically.

Best Practice - Allow IPS to activate protections based on the IPS policy in the beginning. During this time, you can analyze the alerts that IPS generates and how it handles network traffic, while you minimize the impact on the flow of traffic. Then you can manually change the protection settings to suit your needs.

In the Threat Prevention profile, you can configure an updates policy for IPS protections that were newly updated. You can do this with the **IPS** > **Updates** page in the **Profiles** navigation tree. Select one of these settings for **Newly Updated Protections**:

- **Active - According to profile settings -** Protections are activated according to the settings in the **General** page of the Profile. This option is selected by default.

  Set activation as staging mode - Selected by default. Newly updated protections will remain in staging mode until you change their configuration. The default action for the protections is Detect. You can change the action manually in the IPS **Protections** page.

  Click **Configure** to exclude protections from the staging mode.
- **Inactive** - Newly updated protections will not be activated

Configuring Anti-Virus Settings

You can configure Threat Prevention to exclude files from inspection, such as internal emails and internal file transfers. These settings are based on the interface type (internal or external, as defined in SmartConsole) and traffic direction (incoming or outgoing).

Before you define the scope for Threat Prevention, you must make sure that your DMZ interfaces are configured correctly. To do this:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Network Management** and then double-click a DMZ interface.
3. In the **General** page of the **Interface** window, click **Modify**.
4. In the **Topology Settings** window, click **Override** and **Interface leads to DMZ**.
5. Click **OK** and close the gateway window.
   Perform this procedure for each interface that goes to the DMZ.

To configure Anti-Virus settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **Anti-Virus**.
5. Select the Anti-Virus **UserCheck Settings** options:
   - **Prevent** - Select the UserCheck message that opens for a **Prevent** action.
   - **Ask** - Select the UserCheck message that opens for an **Ask** action.

6. In the **Protected Scope** section, select an interface type and traffic direction option:
   - **Inspect incoming files from**:

     Sends **only incoming** files from the specified interface type for inspection. Outgoing files are not inspected. Select an interface type from the list:

     - **External** - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.
     - **External and DMZ** - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
     - **All** - Inspect all incoming files from all interface types.
   - **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection.
7. Select the applicable **Protocols** that Anti-Virus scans:
   - **HTTP**
   - **Mail (SMTP)** - Click **Mail** to configure the SMTP traffic inspection. This links you to the **Mail** page in the.
8. Select **File Types**:
   - **Process file types known to contain malware**
   - **Process all file types -** Select **Enable deep inspection scanning**, if needed. Remember, it impacts performance.
   - **Process specific file types families**
9. To configure the specific file type families:

   a) Click **Configure**.

   b) In the **File Types Configuration** window, for each file type, select the Anti-Virus action for the file type.

   c) Click **OK** to close the **File Types Configuration** window.
10. **Archives** - You can configure the Anti-Virus profile to enable **archive scanning** ("Enabling Archive Scanning" on page 197).
11. Click **OK** and close the Threat Prevention profile window.
12. **Install Policy**.

Enabling Archive Scanning

You can configure the Anti-Virus settings to enable archive scanning. The Anti-Virus engine unpacks archives and applies proactive heuristics. The use of this feature impacts network performance.

Select **Enable Archive scanning (impacts performance)** and click **Configure:**

1. **Stop processing archive after (seconds)** - Sets the amount in seconds to stop processing the archive. The default is 30 seconds.
2. **When maximum time is exceeded (action on file)** - Sets to block or allow the file when the time for processing the archive is exceeded. The default setting is **Allow**.

Blocking Viruses

To block viruses and malware in your organization:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
2. In the **General Properties** page, select the **Anti-Virus** Software Blade.
   The **First Time Activation** window opens.
3. Select **According to the Anti-Bot and Anti-Virus policy** and click **OK**.
4. Close the gateway Properties window and publish the changes.
5. Click **Security Policies** > **Threat Prevention** > **Policy** > **Threat Prevention**.
6. Click **Add Rule**.
   A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
7. Make a rule that includes these components:
   - **Name** - Give the rule a name such as **Block Virus Activity**.
   - **Protected Scope -** The list of network objects you want to protect. In this example, the **Any** network object is used.
   - **Action -** The Profile that contains the protection settings you want. The default profile is **Optimized**.
   - **Track -** The type of log you want to get when detecting malware on this scope. In this example, keep **Log** and also select **Packet Capture** to capture the packets of malicious activity. You will then be able to view the actual packets in **SmartConsole > Logs & Monitor > Logs**.
   - **Install On** - Keep it as **All** or choose specified gateways to install the rule on.
8. Install the Threat Prevention policy.

Configuring Anti-Bot Settings

To configure the Anti-Bot settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **Anti-Bot**.
5. Configure the Anti-Bot **UserCheck Settings**:
   - **Prevent** - Select the UserCheck message that opens for a **Prevent** action
   - **Ask** - Select the UserCheck message that opens for an **Ask** action
6. Click **OK** and **Install Policy**.

Blocking Bots

To block bots in your organization, install this default Threat Policy rule that uses the Optimized profile, or create a new rule.

Protected Scope	Action	Track	Install On
Any	Optimized	Log Packet Capture	Policy Targets

To block bots in your organization:

1. In SmartConsole, click **Gateways & Servers**.
2. Enable the **Anti-Bot** Software Blade on the Gateways that protect your organization. For each Gateway:
   a) Double-click the Gateway object.
   b) In the **Gateway Properties** page, select the **Anti-Bot** Software Blade.
      The First Time **Activation** window opens.
   c) Select **According to the Anti-Bot and Anti-Virus policy**
   d) Click **OK**.
3. Click **Security Policies > Threat Prevention > Policy > Threat Prevention**.
   You can block bots with the out-of-the-box Threat Prevention policy rule with the default **Optimized** Profile.
   Alternatively, add a new Threat Prevention rule:
   a) Click **Add Rule**.
      A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
   b) Make a rule that includes these components:
      - **Name** - Give the rule a name such as **Block Bot Activity**.
      - **Protected Scope -** The list of network objects you want to protect. By default, the **Any** network object is used.
      - **Action -** The Profile that contains the protection settings you want. The default profile is **Optimized**.
      - **Track -** The type of log you want to get when the gateway detects malware on this scope.
      - **Install On** - Keep it as **Policy Targets** or select Gateways to install the rule on.
4. Install the Threat Prevention policy (see "Installing the Threat Prevention Policy" on page 188).

Monitoring Bot Activity

Scenario: I want to monitor bot activity in my organization without blocking traffic at all. How can I do this?

In this example, you will create this Threat Prevention rule, and install the Threat Prevention policy:

Name	Protected Scope	Action	Track	Install On
Monitor bot activity	Any	A profile that has **these** changes relative to the **Optimized** profile: **Confidence** (High\Medium\Low): **Detect\Detect\Detect**	Log	Policy Targets

To monitor all bot activity:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. Create a new profile:
   a) From the **Threat Tools** section, click **Profiles**.
      The **Profiles** page opens.
   b) Right-click a profile and select **Clone**.
   c) Give the profile a name such as **Monitoring_Profile**.
   d) Edit the profile, and under **Activation Mode**, configure all confidence level settings to **Detect**.
   e) Select the **Performance Impact** - for example, **Medium or lower**.

   This profile detects protections that are identified as an attack with low, medium or high confidence and have a medium or lower performance impact.
3. Create a new rule:
   a) Click **Threat Prevention > Policy > Threat Prevention**.
   b) Add a rule to the Rule Base.
      The first rule that matches is applied.
   c) Make a rule that includes these components:
      - **Name** - Give the rule a name such as **Monitor Bot Activity**.
      - **Protected Scope -** Keep **Any** so the rule applies to all traffic in the organization.
      - **Action -** Right-click in this cell and select **Monitoring_Profile**.
      - **Track -** Keep **Log**.
      - **Install On** - Keep it as **Policy Targets** or choose Gateways to install the rule on.
4. Install the Threat Prevention policy (see "Installing the Threat Prevention Policy" on page 188).

Disabling a Protection on One Server

Scenario: The protection Backdoor.Win32.Agent.AH blocks malware on windows servers. How can I change this protection to **detect** *for one server only?*

In this example, create this Threat Prevention rule, and install the Threat Prevention policy:

Name	Protected Scope	Protection/Site	Action	Track	Install On
Monitor Bot Activity	Any	- N/A	A profile based on the Optimized profile, with these changes: **Confidence** (Low/Medium/High): Prevent/Prevent/Prevent	Log	Policy Targets
Exclude	Server_1	Backdoor.Win32.Agent.AH	Detect	Log	Server_1

To add an exception to a rule:

1. In SmartConsole, click **Threat Prevention > Policy > Layer**.
2. Click the rule that contains the scope of Server_1.
3. Click the **Add Exception** toolbar button to add the exception to the rule. The gateway applies the first exception matched.
4. Right-click the rule and select **New Exception**.
5. Configure these settings:
   - **Name** - Give the exception a name such as **Exclude**.
   - **Protected Scope -** Change it to **Server_1** so that it applies to all detections on the server.
   - **Protection/Site** - Click **+** in the cell. From the drop-down menu, click the category and select one or more of the items to exclude.

     Note - To add EICAR files as exceptions, you must add them as Whitelist Files. When you add EICAR files through Exceptions in Policy rules, the gateway still blocks them, if archive scanning is enabled.
   - **Action -** Keep it as **Detect**.
   - **Track** - Keep it as **Log**.
   - **Install On** - Keep it as **Policy Targets** or select specified gateways to install the rule on.
6. **Install Policy**.

Configuring Threat Emulation Settings

Before you define the scope for Threat Prevention, you must make sure that your DMZ interfaces are configured correctly. To do this:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Network Management** and then double-click a DMZ interface.
3. In the **General** page of the **Interface** window, click **Modify**.
4. In the **Topology Settings** window, click **Override** and **Interface leads to DMZ**.

5. Click **OK** and close the gateway window.

Do this procedure for each interface that goes to the DMZ.

If there is a conflict between the Threat Emulation settings in the profile and for the Security Gateway, the profile settings are used.

To configure Threat Emulation settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **Threat Emulation > General**.
5. Select the Threat Emulation **UserCheck Settings** options:
   - **Prevent** - Select the UserCheck message that opens for a **Prevent** action
   - **Ask** - Select the UserCheck message that opens for an **Ask** action
6. In the **Protected Scope** section, select an interface type and traffic direction option:
   - **Inspect incoming files from**:

     Sends **only incoming** files from the specified interface type for inspection. Outgoing files are not inspected. Select an interface type from the list:

     - **External** - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.
     - **External and DMZ** - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
     - **All** - Inspect all incoming files from all interface types.
   - **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection.
7. Select the applicable **Protocols** to be emulated.
   - **HTTP**
   - **Mail (SMTP)** - Click **Mail** to configure the SMTP traffic inspection by the Threat Emulation blade. This links you to the **Mail** tab in the Profile.
8. Select the **File Types** to be emulated.
9. **Archives** - **Block archives containing these prohibited file types**. Click **Configure** to select the prohibited file types. If a prohibited file type is in an archive, the gateway drops the archive.
10. Click **OK** and close the Threat Prevention profile window.
11. Install the Threat Prevention policy.

Selecting the Threat Emulation Action

What are the available emulation actions that I can use with a Threat Emulation profile?

- **Prevent** - Files do not go to the destination computer until emulation is completed. If Threat Emulation discovers that a file contains malware, the malicious file does not enter the internal network. Users can notice a delay when downloading a file, because they cannot download and open the file until the emulation is complete.
- **Detect** - The file is sent to the destination and to Threat Emulation. If Threat Emulation discovers that a file contains malware, the appropriate log action is done. Users receive all files without delay.

- **Note** - To estimate the system requirements and amount of file emulations for a network, go to sk93598 http://supportcontent.checkpoint.com/solutions?id=sk93598.

Configuring the Virtual Environment (Profile)

You can use the **Emulation Environment** window to configure the emulation location and images that are used for this profile.

The **Analysis Locations** section lets you select where the emulation is done.

The **Environments** section lets you select the operating system images on which the emulation is run. If the images defined in the profile and the Security Gateway or Emulation appliance are different, the profile settings are used.

These are the options to select the emulation images:

- Check Point automatically updates images and adds new ones.
- Select the images that are closest to the operating systems for the computers in your organization.

To configure the virtual environment settings for the profile:

1. From the Threat Prevention profile navigation tree, select **Threat Emulation** > **Emulation Environment**.

   The **Emulation Environment** page opens.
2. Set the **Analysis Location** setting:
   - To use the Security Gateway settings for the location of the virtual environment, click **According to the gateway**
   - To configure the profile to use a different location of the virtual environment, click **Specify** and select the applicable option
3. Set the **Environments** setting:
   - To use the emulation environments recommended by Check Point security analysts, click **Use Check Point recommended emulation environments**
   - To select one or more images that are used for emulation, click **Use the following emulation environments**
4. Click **OK** and close the Threat Prevention profile window.
5. Install the Threat Prevention policy.

Excluding Emails

You can enter email addresses that are not included in the Threat Emulation protection. SMTP traffic that is sent to or from these addresses is not sent for emulation.

Note - If you want to do emulation on outgoing emails, make sure that you set the Protected Scope to **Inspect incoming and outgoing files**.

To exclude emails from the Threat Emulation protection:

1. From the Threat Prevention profile navigation tree, go to the **Mail** tab > **Exceptions** > **Emulation Exceptions**.
2. Click **Configure**.
3. In the **Recipients** section, you can click the Add button and enter one or more emails.

   Emails and attachments that are sent to these addresses will not be sent for emulation.

4. In the **Senders** section, you can click the Add button and enter one or more emails.

   Emails and attachments that are received from these addresses will not be sent for emulation.

   Note - You can also use a wildcard character to exclude more than one email address from a domain.
5. Click **OK** and close the Threat Prevention profile window.
6. Install the Threat Prevention policy.

Preparing for Local or Remote Emulation

Prepare the network and Emulation appliance for a Local or Remote deployment in the internal network.

1. Open SmartConsole.
2. Create the network object for the Emulation appliance.
3. If you are running emulation on HTTPS traffic, configure the settings for HTTPS Inspection.
4. Make sure that the traffic is sent to the appliance according to the deployment:
   - Local Emulation - The Emulation appliance receives the traffic. The appliance can be configured for traffic the same as a Security Gateway.
   - Remote Emulation - The traffic is routed to the Emulation appliance.

Configuring Threat Extraction Settings

To configure Threat Extraction settings for a Threat Prevention profile:

1. In the **Security Policies** view > **Threat Tools** section, click **Profiles**.
2. Right-click a profile and select **Edit**.

   The **Profiles** properties window opens.
3. On the **General Policy** page in the **Blade Activation** area, select **Threat Extraction**.
4. Configure these Threat Extraction Settings:
   - **General**
   - **Advanced**.
5. Click **OK**.

Note - You can configure some of the Threat Extraction features in a configuration file, in addition to the CLI and GUI. See sk114613 http://supportcontent.checkpoint.com/solutions?id=sk114613.

Configuring Threat Extraction on the Security Gateway

1. In the **Gateways & Servers** view, open the **gateway properties** > **Threat Extraction** page.
2. Set the **Activation Mode** to **Active**.
3. In the **Resource Allocation** section, configure the resource settings.
4. Click **OK**.
5. **Install Policy**.

Configuring a Malware DNS Trap

The Malware DNS trap works by configuring the Security Gateway to return a false (bogus) IP address for known malicious hosts and domains. You can use the Security Gateways external IP address as the DNS trap address but:

- Do not use a gateway address that leads to the internal network
- Do not use the gateway internal management address
- If the gateway external IP address is also the management address, select a different address for the DNS trap.

You can also add internal DNS servers to better identify the origin of malicious DNS requests.

Using the Malware DNS Trap you can detect compromised clients by checking logs with connection attempts to the false IP address.

At the Security Gateway level, you can configure the DNS Trap according to the profile settings or as a specific IP address for all profiles on the specific gateway.

To set the Malware DNS Trap parameters for the profile:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **Malware DNS Trap**.
5. Click **Activate DNS Trap**.
6. Enter the **IP** address for the DNS trap.
7. **Optional:** Add **Internal DNS Servers** to identify the origin of malicious DNS requests.
8. Click **OK** and close the Threat Prevention profile window.
9. Install the Threat Prevention policy.

To set the Malware DNS Trap parameters for a gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, select **Anti-Bot and Anti-Virus**.
3. In the **Malicious DNS Trap** section, select one of these options:
   - **According to profile settings** - Use the Malware DNS Trap IP address configured for each profile.
   - **IPv4** - Enter an IP address to be used in all the profiles assigned to this Security Gateway.
4. Click **OK**.
5. Install the policy.

Exception Rules

If necessary, you can add an **exception** directly to a rule. The object in the **Protected Scope** column can have a different **Action** from the specified Threat Prevention rule. Here are some examples of exception rules:.

- A profile that only detects protections. You can set one or more of the protections for a user to **Prevent**.
- The Research and Development (R&D) network protections are included in a profile with the **Prevent** action. You can set that network to **Detect**.

You can add one or more exceptions to a rule. The exception is added as a shaded row below the rule in the Rule Base. It is identified in the **No.** column with the rule's number plus the letter E and a digit that represents the exception number. For example, if you add two exceptions to rule number 1, two lines will be added and show in the Rule Base as E-1.1 and E-1.2.

You can use exception groups to group exceptions that you want to use in more than one rule. See the Exceptions Groups Pane.

You can expand or collapse the rule exceptions by clicking on the minus or plus sign next to the rule number in the **No**. column.

To add an exception to a rule:

1. In the **Policy** pane, select the rule to which you want to add an exception.
2. Click **Add Exception.**
3. Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4. Enter values for the columns. Including these:
   - **Protected Scope -** Change it to reflect the relevant objects.
   - **Protection** - Click the plus sign in the cell to open the Protections viewer. Select the protection(s) and click **OK**.
5. **Install Policy**.

Note - You cannot set an exception rule to an inactive protection or an inactive blade.

Blade Exceptions

You can also configure an exception for an entire blade.

To configure a blade exception:

1. In the **Policy,** select the Layer rule to which you want to add an exception.
2. Click **Add Exception**.
3. Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4. In the **Protection/Site** column, select **Blades** from the drop-down menu.
5. Select the blade you want to exclude.
6. **Install Policy**.

The Check Point ThreatCloud

In This Section:

Check Point ThreatCloud is a dynamically updated service that is based on an innovative global network of threat sensors and organizations that share threat data and collaborate to fight against modern malware. Customers can send their own threat data to the ThreatCloud and benefit from increased security and protection and enriched threat intelligence. The ThreatCloud distributes attack information, and turns zero-day attacks into known signatures that the Anti-Virus Software Blade can block. The Security Gateway does not collect or send any personal data.

Participation in Check Point information collection is a unique opportunity for Check Point customers to be a part of a strategic community of advanced security research. This research aims to improve coverage, quality, and accuracy of security services and obtain valuable information for organizations.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

For the reputation and signature layers of the ThreatSpect engine, each Security Gateway also has:

- A local database, the Malware database that contains commonly used signatures, URLs, and their related reputations. You can configure automatic or scheduled updates for this database.
- A local cache that gives answers to 99% of URL reputation requests. When the cache does not have an answer, it queries the ThreatCloud repository.
  - For Anti-Virus - the signature is sent for file classification.
  - For Anti-Bot - the host name is sent for reputation classification.

Access the ThreatCloud repository from:

- **SmartConsole** - You can add specific malwares to rule exceptions when necessary. From the Threat Prevention Rule Base in SmartConsole, click the plus sign in the **Protection** column in the rule exceptions, and the Protection viewer opens.
- **Threat Wiki** - A tool to see the entire Malware database. Open Threat Wiki in SmartConsole or access it from the Check Point website.

Data Check Point Collects

When you enable information collection, the Check Point Security Gateway collects and securely submits event IDs, URLs, and external IPs to the Check Point Lab regarding potential security risks.

For example:

```
<entry engineType="3" sigID="-1" attackName="CheckPoint - Testing Bot"
sourceIP="7a1ec646fe17e2cd" destinationIP="d8c8f142" destinationPort="80"
host="www.checkpoint.com"
path="/za/images/threatwiki/pages/TestAntiBotBlade.html"
numOfAttacks="20" />
```

This is an example of an event that was detected by a Check Point Security Gateway. It includes the event ID, URL, and external IP addresses. Note that the data does not contain confidential data or internal resource information. The source IP address is obscured. Information sent to the Check Point Lab is stored in an aggregated form.

Updating IPS Protections

Check Point constantly develops and improves its protections against the latest threats. You can immediately update IPS with real-time information on attacks and all the latest protections. You can manually update the IPS protections and also set a schedule when updates are automatically downloaded and installed. IPS protections include many protections that can help manage the threats against your network. Make sure that you understand the complexity of the IPS protections before you manually modify the settings.

Note - To enforce the IPS updates, you must install policy.

To update IPS Protections:

1. In SmartConsole, click **Security Policies** > **Threat Prevention**.
2. In the **Threat Tools** section, click **Updates**.
3. In the **IPS** section > **Update Now**, from the drop-down menu, select:
   - Download with SmartConsole (if your Security Management Server has no internet access), or
   - Download with Security Management Server.
4. **Install Policy**.

Note - From R80.20, IPS purge runs automatically after every IPS update. The Security Management Server saves only the versions from the last 30 days, and deletes the others.

Scheduling Updates

You can change the default automatic schedule for when updates are automatically downloaded and installed. If you have Security Gateways in different time zones, they are not synchronized when one updates and the other did not yet update.

To configure Threat Prevention scheduled updates:

1. In SmartConsole, go to the **Security Policies** page and select **Threat Prevention**.
2. In the **Threat Tools** section of the Threat Prevention Policy, click **Updates**.
3. In the section for the applicable Software Blade, click **Schedule Update**.
   The **Scheduled Update** window opens.
4. Make sure **Enable <feature> scheduled update** is selected.
5. Click **Configure**.
6. In the window that opens, set the **Update at** time and the frequency:
   - **Daily** - Every day
   - **Days in week** - Select days of the week
   - **Days in month** - Select dates of the month
7. Optional, for IPS only:
   - Select **Perform retries on update failure -** lets you configure how many tries the Scheduled Update makes if it does not complete successfully the first time.

- Select **On successful update perform Install Policy** - automatically installs the policy on the devices you select after the IPS update is completed. Click **Configure** to select these devices.

8. Click **OK**.
9. Click **Close**.
10. **Install Policy**.

Updating Threat Emulation

Threat Emulation connects to the ThreatCloud to update the engine and the operating system images. The default setting for the Threat Emulation appliance is to automatically update the engine and images.

The default setting is to download the package once a day.

Best Practice - Configure Threat Emulation to download the package when there is low network activity.

Update packages for the Threat Emulation operating system images are usually more than 2GB. The actual size of the update package is related to your configuration.

To enable or disable Automatic Updates for Threat Emulation:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Updates**.
   The **Updates** page opens.
3. Under Threat Emulation, click **Schedule Update**.
4. Select or clear these settings:
   - **Enable Threat Emulation engine scheduled update**
   - **Enable Threat Emulation images scheduled update**
5. Click **Configure** to configure the schedule for Threat Emulation engine or image updates.
6. Configure the automatic update settings to update the database:
   - To update once a day, select **At** and enter the time of day
   - To update multiple times a day, select **Every** and set the time interval
   - To update once or more for each week or month:

   a) Select **At** and enter the time of day.

   b) Click **Days**.

   c) Click **Days of week** or **Days of month**.

   d) Select the applicable days.
7. Click **OK** and then install the Threat Prevention policy.

To Learn More About Threat Prevention

To learn more about configuring a Threat Prevention Policy, see the *R80.10 Threat Prevention Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54828.

Managing User Accounts

In This Section:

Authentication Methods for Users and Administrators

Check Point supports different methods of authenticating end users and administrators.

Security Gateways authenticate individual users. The Security Management Server authenticates administrators.

Users and Administrators authenticate using credentials. All the methods required a username and password.

Users and administrators can be stored in the Check Point User Database (on page 215) or on an LDAP server.

The following sections describe the supported authentication methods.

Check Point Password

Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Security Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.

Operating System Password

OS Password is stored on the operating system of the computer on which the Security Gateway (for users) or Security Management Server (for administrators) is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server.

Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication.

The RADIUS protocol uses UDP to communicate with the gateway or the Security Management Server.

RADIUS servers and RADIUS server group objects are defined in SmartConsole.

SecurID

SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA ACE/server and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the ACE/server.

Using SecurID, the Security Gateway forwards authentication requests by remote users to the ACE/server. For administrators, it is the Security Management Server that forwards the requests. ACE manages the database of RSA users and their assigned hard or soft tokens. The gateway or the Security Management Server act as an ACE/Agent 5.0 and direct all access requests to the RSA ACE/server for authentication. For additional information on agent configuration, refer to ACE/server documentation.

There are no specific parameters required for the SecurID authentication method.

TACACS

Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers.

TACACS is an external authentication method that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. For administrators, it is the Security Management Server that forwards the requests. The TACACS server, which stores user account information, authenticates users. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

Configuring Authentication Methods for Users

These instructions show how to configure authentication methods for users. For administrators, see Configuring Authentication Methods for Administrators (on page 39).

For background information about the authentication methods, see Authentication Methods for Users and Administrators (on page 210).

Granting User Access Using RADIUS Server Groups

The Security Gateway lets you control access privileges for authenticated RADIUS (on page 210) users, based on the administrator's assignment of users to RADIUS groups. These groups are used in the Security Rule Base to restrict or give users access to specified resources. Users are unaware of the groups to which they belong.

To use RADIUS groups, you must define a return attribute in the RADIUS user profile of the RADIUS server. This attribute is returned to the Security Gateway and contains the group name (for example, **RAD_<group to which the RADIUS users belong>**) to which the users belong.

Use these RADIUS attributes (refer to RFC 2865):

- For SecurePlatform - attribute "Class" (25)
- For other operating systems, including Gaia, Windows, and IPSO-attribute "Vendor-Specific" (26)

Configuring a Security Gateway to use SecurID Authentication

Sample workflow for SecurID (on page 211) authentication configuration:

1. Configure gateways for SecurID authentication.
2. Define user groups.
3. Configure SecurID authentication settings for users.

   The procedure for doing this is different for Internal Users (that are defined in the internal User Database on the Security Management Server) and for External Users.
4. Complete the SecurID authentication configuration.

To configure a Security Gateway to use SecurID:

1. Generate the *sdconf.rec* file on the ACE/Server and copy it to:
   - `/var/ace/sdconf.rec` on UNIX, Linux or IPSO
   - `%SystemRoot%\System32\sdconf.rec` on 32-bit Windows
   - `%SystemRoot%\SysWOW64\sdconf.rec` on 64-bit Windows

   On a Virtual System, follow the instructions in sk97908 http://supportcontent.checkpoint.com/solutions?id=sk97908.
2. In SmartConsole, go to the **Gateways & Servers** view, right-click a Security Gateway object and select **Edit**.
3. In the gateway property window that opens, select **Other** > **Legacy Authentication**.
4. In the **Enabled Authentication Schemes** section, select **SecurID**.
5. Click **OK**.

To define a user group:

1. In SmartConsole, open the **Objects Bar (F11)**.
2. Click **New** > **More** > **User** > **User Group**.

   The **New User Group** window opens.
3. Enter the name of the group, for example *SecurID_Users*.

   Make sure the group is empty.
4. Click **OK**.
5. Publish the changes and install the policy.

To configure SecurID authentication settings for Internal Users:

Internal users are users that are defined in the internal User Database on the Security Management Server.

1. Create a new user. In SmartConsole, open the **Objects Bar (F11)**.
2. Click **New** > **More** > **User** > **User**.

   The **New User** window opens.
3. Choose a template.

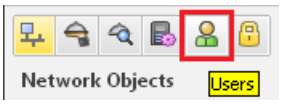
4. Click **OK**.
5. In the **General** page:
   - Enter a default **Name**. This name will be used to authenticate users on the ACE/Server.
   - Set the **Expiration** date.
6. In the **Authentication** page, from the **Authentication Method** drop-down list, select **SecurID.**
7. Click **OK**.

To configure SecurID authentication settings for External Users:

External users are users that are not defined in the internal Users Database on the Security Management Server.

1. In SmartConsole, click **Manage & Settings** > **Blades**.
2. In the **Mobile Access** section, click **Configure in SmartDashboard**.

   Legacy SmartDashboard opens.
3. In the bottom left Network Objects pane, and click **Users**.



4. Right-click on an empty space and select the applicable option:
   - If you support only one external authentication scheme, select **New** > **External User Profile > Match all users**.
   - If you support more than one external authentication scheme, select **New** > **External User Profile > Match by domain**.
5. Configure the **External User Profile** properties:

   a) **General Properties** page:

   - If selected **Match all users**, then configure:

     In the **External User Profile name** field, leave the default name `generic*`.

     In the **Expiration Date** field, set the applicable date.
   - If selected **Match by domain**, then configure:

     In the **External User Profile name** field, enter the applicable name. This name will be used to authenticate users on the ACE/Server.

     In the **Expiration Date** field, set the applicable date.

     In the **Domain Name matching definitions** section, configure the applicable settings.

   b) **Authentication** page:

   From the **Authentication Scheme** drop-down list, select **SecurID.**

   c) Click **OK**.
6. From the top toolbar, click **Update** (Ctrl + S).
7. Close the Legacy SmartDashboard.

To complete the SecurID authentication configuration:

1. Make sure that connections between the gateway and the ACE/Server are not NATed in the Address Translation Rule Base.

   On a Virtual System, follow the instructions in sk107281 http://supportcontent.checkpoint.com/solutions?id=sk107281.
2. Save, verify, and install the policy in SmartConsole.

When a Security Gateway has multiple interfaces, the SecurID agent on the Security Gateway sometimes uses the wrong interface IP to decrypt the reply from the ACE/Server, and authentication fails.

To overcome this problem, place a new text file, named `sdopts.rec` in the same directory as `sdconf.rec`. The file should contain the `CLIENT_IP=<ip>` line, where *<ip>* is the primary IP address of the Security Gateway, as defined on the ACE/Server. This is the IP address of the interface to which the server is routed.

Configuring TACACS+ Authentication

To configure a Security Gateway to use TACACS+ authentication, you must set up the server and enable its use on the Security Gateway.

To define a TACACS+ server:

1. Define a TACACS Host object: **Object Explorer** (Ctrl+E) > **New** > **Host**
2. Enter a name and IP address.
3. Define a TACACS server: **Object Explorer** (Ctrl+E) > **New** > **Server** > **More** > **TACACS**.
4. Enter a name.
5. In **Host**, select the TACACS host.
6. Select the **Type**.

   Best Practice: The default is **TACACS**, but **TACACS+** is recommended.
7. In **Service**, select the **TACACSplus** service (or **TACACS** UDP service if you selected **TACACS** type).
8. Enter a **Secret key**. (If you selected **TACACS** type, this is not available. If you selected **TACACS+**, it is required.)
9. Click **OK**.

To enable TACACS on the Security Gateway:

1. Right-click the gateway object and select **Edit**.
2. Click **Other** > **Legacy Authentication**.
3. In the **Enabled Authentication Schemes** section, click **TACACS**.
4. Click **OK**.

To enable TACACS authentication for users:

1. In the Object Explorer, click **Users** > **User Templates**.
2. Edit the **Default** user template.
3. In the **Authentication** page, **Authentication method** list, select **TACACS**.
4. When **TACACS server** shows, select the TACACS server you defined.
5. Click **OK**.

   When you create a new user account, TACACS is the default selected authentication.

User Database

Users defined in SmartConsole are saved to the *User Database* on the Security Management Server, together with the user authentication schemes and encryption keys. Then, the user database is installed on Security Gateways and Check Point hosts:

- On Security Gateways - When the policy is installed (**Install Policy**)
- On Check Point hosts with an active Management blade (such as Log Server) - When the database is installed (**Install Database**)

The user database does *not* contain information about users defined elsewhere than on the Security Management Server (such as users in external User Directory groups), but it does contain information about the external groups themselves (for example, on which Account Unit the external group is defined). Changes to external groups take effect only after the policy is installed, or the user database is downloaded from the management server.

Creating, Modifying, Removing User Accounts

To create a new user:

1. In the **Object Bar** (F11)tree, click **New** > **More** > **User** > **User**.
   The **New User** window opens.
2. Choose a template and click **OK**.
3. Configure required and optional settings in General Properties ("User > General Properties" on page 215).
4. Select and configure Authentication ("User > Authentication" on page 216).
   Important! If you do not select an authentication method, the user cannot log in or use network resources.
5. In Location ("User > Location" on page 216), select objects from which this user can access or send data and traffic.
6. If the user has specified working days or hours, configure *when ("User > Time" on page 216)* the user can be authenticated for access.
7. Click **OK**.

To change an existing user:

1. In the object tree, click **Users** > **Users**.
2. Double-click a user.
   The **User Properties** window opens.
3. Change the properties as necessary.
4. Click **OK**.

User > General Properties

Required settings:

- **User Name** - A unique, case sensitive character string.
  If you generate a user certificate with a non-Check Point Certificate Authority, enter the Common Name (CN) component of the Distinguished Name (DN). For example, if the DN is: [CN = James, O = My Organization, C = My Country],

enter `James` as the user name. If you use Common Names as user names, they must contain exactly one string with no spaces.

- **Expiration Date** - The date, after which the user is no longer authorized to access network resources and applications. By default, the date defined in the Default Expiration Settings ("Configuring Default Expiration Settings for Users" on page 217) shows as the expiration date.

Optional settings:

- **Comment**
- **Email Address**
- **Mobile Phone Number**

User > Authentication

Select an **Authentication Scheme**:

- **SecurID**
- **Check Point Password** - Enter the password string (between 4 and 8 characters) and confirm it
- **OS Password**
- **RADIUS** - Select a RADIUS server or a group of servers
- **TACACS** - Select a TACACS server

User > Location

In the **Allowed locations** section:

Source - Click **Add**, to add selected objects to this user's permitted resources. The user can get data and traffic from these objects.

Destination - Click **Add**, to add selected objects to this user's permitted destinations. The user can send data and traffic to these objects.

User > Time

From and **To** - Enter start time and end time of an expected workday. This user will not be authenticated if a login attempt is made on a time outside the given range.

Days in week or **Daily** - Select the days that the user can authenticate and access resources. This user will not be authenticated if a login attempt is made on an unselected day.

User > Certificates

Generate and register SIC certificates for user accounts. This authenticates the user in the Check Point system. Use certificates with required authentication for added access control.

To create a new certificate:

1. Open the **User Properties** window > **Certificates** page.
2. Click **New**.
3. Select key or `p12` file:
   - **Registration key for certificate enrollment** - Select to send a registration key that activates the certificate. When prompted, select the number of days the user has to activate the certificate, before the registration key expires.

- **Certificate file (p12)** - Select to create a `.p12` certificate file with a private password for the user. When prompted, enter and confirm the certificate password.

4. Click **OK**.

If a user will not be in the system for some time (for example, going on an extended leave), you can revoke the certificate. This leaves the user account in the system, but it cannot be accessed until you renew the certificate.

To revoke a certificate, select the certificate and click **Revoke**.

User > Encryption

If the user will access resources from a remote location, traffic between the remote user and internal resources will be encrypted. Configure encryption settings for remote access users.

To configure encryption:

1. Open the **User Properties** window > **Encryption** page.
2. Select an encryption method for the user.
3. Click **Edit**.

   The encryption **Properties** window opens.

   The next steps are for **IKE Phase 2**. The options can be different for different methods.
4. Open the **Authentication** tab.
5. Select the authentication schemes:

   a) **Password** - The user authenticates with a pre-shared secret password. Enter and confirm the password.

   b) **Public Key** - The user authenticates with a public key contained in a certificate file.
6. Click **OK**.
7. Click **OK**.

Configuring Default Expiration Settings for Users

If a user account is about to expire, notifications show when you open the properties of the user in SmartConsole.

To configure the default expiration settings:

1. From the **Menu**, select **Global Properties**.

   The **Global Properties** window opens.
2. Click **User Accounts**.
3. Select **Expire at** or **Expire after**.
   - **Expire at** - Select the expiration date from the calendar control.
   - **Expire after** - Enter the number of days (from the day the account is made) before user accounts expire.
4. Select **Show accounts expiration indication**, and enter the number of days.

   Expiration warnings in the SmartConsole User object show this number of days before an account expires. During this time, if the user account is to be active for longer, you can edit the user account expiration configuration. This will avoid loss of working time.

Delete a User

To delete a user:

1. In the object tree, click **Users** > **Users**.
2. Right-click the account and select **Delete**.
   The confirmation window opens.
3. Click **Yes**.

Managing User Groups

User groups are collections of user accounts. Add the user group to the *Source* or *Destination* of a rule. You cannot add individual users to a rule.

You can also edit user groups, and delete user groups that are not used in the Rule Base.

Adding User Groups

To create a new user group:

1. In the **Object Bar** (F11), click **New> More > User > User Group**.
   The **New User Group** window opens.
2. Enter a name for the new group.
3. For each user or a group of users, click the [**+**] sign and select the object from the list.
4. Configure the optional settings:
   - **Mailing List Address**
   - **Comment**
   - **Tag**
   - **Color**
5. Click **OK**.

To add new users or other user groups to a group:

1. In the **Object Bar** (F11), select **Object Categories** > **User** >**User Groups**
2. Right click the User group and click **Edit**.
   The **User Group** window opens.
3. Click **+**
4. Select users or user groups.
5. Click **OK**.

LDAP and User Directory

Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution. If you have a large user count, we recommend that you use an external user management database such as LDAP for enhanced Security Management Server performance.

- Users can be managed externally by an LDAP server.
- The gateways can retrieve CRLs.

- The Security Management Server can use the LDAP data to authenticate users.
- User data from other applications gathered in the LDAP user database can be shared by different applications.

You can choose to manage Domains on the Check Point users database, or to implement an external LDAP server.

Note - User Directory requires a special license. If you have the Mobile Access Software Blade, you have the User Directory license.

User Directory lets you configure:

- *High Availability*, to duplicate user data across multiple servers for backup (see "Account Units and High Availability" on page 246).
- *Multiple Account Units*, for distributed databases.
- *Define LDAP Account Units*, for encrypted User Directory connections (see "Modifying the LDAP Server" on page 246).
- *Profiles*, to support multiple LDAP vendors (see "User Directory Profiles" on page 227).

User Directory and Identity Awareness

Identity Awareness uses User Directory.

Identity Awareness lets you enforce network access and audit data, based on network location, the identity of the user, and the identity of the computer. You can use Identity Awareness in the Access Control, Threat Prevention and DLP Rule Bases.

User Directory Considerations

Before you begin, plan your use of User Directory.

- Decide whether you will use the User Directory servers for user management, CRL retrieval, user authentication ("Working with LDAP Account Units" on page 243), or all of those.
- Decide how many Account Units you will need. You can have one for each User Directory server, or you can divide branches of one User Directory server among different Account Units (on page 243).
- Decide whether you will use High Availability ("Account Units and High Availability" on page 246) setup.
- Determine the order of priority ("Setting High Availability Priority" on page 247) among the User Directory servers for High Availability and querying purposes.
- Assign users ("Managing Users on a User Directory Server" on page 248) to different Account Units, branches, and sub-branches, so that users with common attributes (such as their role in the organization, permissions, etc.) are grouped together.

The User Directory Schema

The User Directory default schema is a description of the structure of the data in a user directory. It has user definitions defined for an LDAP server. This schema does not have Security Management Server or Security Gateway specific data, such as IKE-related attributes, authentication methods, or values for remote users.

You can use the default User Directory schema, if all users have the same authentication method and are defined according to a default template. But if users in the database have different

definitions, it is better to apply a Check Point schema to the LDAP server (see "Check Point Schema for LDAP" on page 220).

In This Section

Check Point Schema for LDAP

The Check Point Schema adds Security Management server and Security Gateway specific data to the structure in the LDAP server. Use the Check Point Schema to extend the definition of objects with user authentication functionality.

For example, an Object Class entitled **fw1Person** is part of the Check Point schema. This Object Class has mandatory and optional attributes to add to the definition of the Person attribute. Another example is **fw1Template**. This is a standalone attribute that defines a template of user information.

Schema Checking

When schema checking is enabled, User Directory requires that every Check Point object class and its associated attributes is defined in the directory schema.

Before you work with User Directory, make sure that schema checking is disabled. Otherwise the integration will fail. After the Check Point object classes and attributes are applied to the User Directory server's schema, you must enable schema checking again.

OID Proprietary Attributes

Each of the proprietary object classes and attributes (all of which begin with "fw1") has a proprietary Object Identifier (OID), listed below.

Object Class OIDs

object class	OID
fw1template	1.3.114.7.4.2.0.1
fw1person	1.3.114.7.4.2.0.2

The OIDs for the proprietary attributes begin with the same prefix ("1.3.114.7.4.2.0.X"). Only the value of "X" is different for each attribute. See Attributes (see "User Directory Schema Attributes" on page 221) for the value of "X".

User Directory Schema Attributes

Attributes:

cn

The entry's name. This is also referred to as "Common Name". For users this can be different from the uid attribute, the name used to login to the Security Gateway. This attribute is also used to build the User Directory entry's distinguished name, that is, it is the RDN of the DN.

uid

The user's login name, that is, the name used to login to the Security Gateway. This attribute is passed to the external authentication system in all authentication methods except for "Internal Password", and must be defined for all these authentication methods.

The login name is used by the Security Management Server to search the User Directory server(s). For this reason, each user entry should have its own unique uid value.

It is also possible to login to the Security Gateway using the full DN. The DN can be used when there is an ambiguity with this attribute or in "Internal Password" when this attribute may be missing. The DN can also be used when the same user (with the same uid) is defined in more than one Account Unit on different User Directory servers.

description

Descriptive text about the user.

default
"no value"

mail

User's email address.

default
"no value"

member

An entry can have zero or more values for this attribute.

- **In a template:** The DN of user entries using this template. DNs that are not users (object classes that are not one of: "person", "organizationalPerson", "inetOrgPerson" or "fw1person") are ignored.
- **In a group:** The DN of user.

userPassword

Must be given if the authentication method (fw1auth-method) is "Internal Password". The value can be hashed using "crypt". In this case the syntax of this attribute is:

"{crypt}xxyyyyyyyyyyy"
where "xx" is the "salt" and "yyyyyyyyyy" is the hashed password.

It is possible (but not recommended) to store the password without hashing. However, if hashing is specified in the User Directory server, you should not specify hashing here, in order to prevent the password from being hashed twice. You should also use SSL in this case, to prevent sending an unencrypted password.

The Security Gateway never reads this attribute, though it does write it. Instead, the User Directory bind operation is used to verify a password.

fw1authmethod

One of these:

RADIUS, TACACS, SecurID, OS Password, Defender

This default value for this attribute is overridden by **Default authentication scheme** in the **Authentication** tab of the **Account Unit** window in SmartConsole. For example: a User Directory

server can contain User Directory entries that are all of the object-class "person" even though the proprietary object-class "fw1person" was not added to the server's schema. If **Default authentication scheme** in SmartConsole is "Internal Password", all the users will be authenticated using the password stored in the "userPassword" attribute.

fw1authserver

"X" in OID	fw1person	fw1template	default
1	y	y	"undefined"

The name of the server that will do the authentication. This field must be given if fw1auth-method is "RADIUS" or "TACACS". For all other values of fw1auth-method, it is ignored. Its meaning is given below:

method	meaning
RADIUS	name of a RADIUS server, a group of RADIUS servers, or "Any"
TACACS	name of a TACACS server

"X" in OID	fw1template
2	y

fw1pwdLastMod

The date on which the password was last modified. The format is `yyyymmdd` (for example, 20 August 1998 is 19980820). A password can be modified through the Security Gateway as a part of the authentication process.

"X" in OID	fw1person	fw1template	default
3	y	y	If no value is given, then the password has never been modified.

fw1expiration-date

The last date on which the user can login to a Security Gateway, or "no value" if there is no expiration date. The format is `yyyymmdd` (for example, 20 August 1998 is 19980820). The default is "no value".

"X" in OID	fw1person	fw1template	default
8	y	y	"no value"

fw1hour-range-from

The time from which the user can login to a Security Gateway. The format is `hh:mm` (for example, 8:15 AM is 08:15).

"X" in OID	fw1person	fw1template	default
9	y	y	"00:00"

fw1hour-range-to

The time until which the user can login to a Security Gateway. The format is `hh:mm` (for example, 8:15 AM is 08:15).

"X" in OID	fw1person	fw1template	default
10	y	y	"23:59"

fw1day

The days on which the user can login to a Security Gateway. Can have the values "SUN","MON", and so on.

"X" in OID	fw1person	fw1template	default
11	y	y	all days of the week

fw1allowed-src

The names of one or more network objects from which the user can run a client, or "Any" to remove this limitation, or "no value" if there is no such client. The names should match the name of network objects defined in Security Management server.

"X" in OID	fw1person	fw1template	default
12	y	y	"no value"

fw1allowed-dst

The names of one or more network objects which the user can access, or "Any" to remove this limitation, or "no value" if there is no such network object. The names should match the name of network objects defined on the Security Management server.

"X" in OID	fw1person	fw1template	default
13	y	y	"no value"

fw1allowed-vlan

Not currently used.

"X" in OID	fw1person	fw1template	default
14	y	y	"no value"

fw1SR-keym

The algorithm used to encrypt the session key in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".

"X" in OID	fw1person	fw1template	default
15	y	y	"Any"

fw1SR-datam

The algorithm used to encrypt the data in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".

"X" in OID	fw1person	fw1template	default
16	y	y	"Any"

fw1SR-mdm

The algorithm used to sign the data in SecuRemote. Can be "none" or "MD5".

"X" in OID	fw1person	fw1template	default
17	y	y	"none"

fw1enc-fwz-expiration

The number of minutes after which a SecuRemote user must re-authenticate himself or herself to the Security Gateway.

"X" in OID	fw1person	fw1template
18	y	y

fw1sr-auth-track

The exception to generate on successful authentication via SecuRemote. Can be "none", "cryptlog" or "cryptalert".

"X" in OID	fw1person	fw1template	default
19	y	y	"none"

fw1groupTemplate

This flag is used to resolve a problem related to group membership.

The group membership of a user is stored in the group entries to which it belongs, in the user entry itself, or in both entries. Therefore there is no clear indication in the user entry if information from the template about group relationship should be used.

If this flag is "TRUE", then the user is taken to be a member of all the groups to which the template is a member. This is in addition to all the groups in which the user is directly a member.

"X" in OID	fw1person	fw1template	default
20	y	y	"False"

fw1ISAKMP-EncMethod

The key encryption methods for SecuRemote users using IKE. This can be one or more of: "DES", "3DES". A user using IKE (formerly known as ISAMP) may have both methods defined.

"X" in OID	fw1person	fw1template	default
21	y	y	"DES", "3DES"

fw1ISAKMP-AuthMethods

The allowed authentication methods for SecuRemote users using IKE, (formerly known as ISAMP). This can be one or more of: "preshared", "signatures".

"X" in OID	fw1person	fw1template	default
22	y	y	"signatures"

fw1ISAKMP-HashMethods

The data integrity method for SecuRemote users using IKE, (formerly known as ISAMP). This can be one or more of: "MD5", "SHA1". A user using IKE must have both methods defined.

"X" in OID	fw1person	fw1template	default
23	y	y	"MD5", "SHA1"

fw1ISAKMP-Transform

The IPSec Transform method for SecuRemote users using IKE, (formerly known as ISAMP). This can be one of: "AH", "ESP".

"X" in OID	fw1person	fw1template	default
24	y	y	"ESP"

fw1ISAKMP-DataIntegrityMethod

The data integrity method for SecuRemote users using IKE, (formerly known as ISAMP). This can be one of: "MD5", "SHA1".

"X" in OID	fw1person	fw1template	default
25	y	y	"SHA1"

fw1ISAKMP-SharedSecret

The pre-shared secret for SecuRemote users using IKE, (formerly known as ISAMP).

The value can be calculated using the `fw ikecrypt` command line.

"X" in OID	fw1person	fw1template
26	y	y

fw1ISAKMP-DataEncMethod

The data encryption method for SecuRemote users using IKE, (formerly known as ISAMP).

"X" in OID	fw1person	fw1template	default
27	y	y	"DES"

fw1enc-Methods

The encryption method allowed for SecuRemote users. This can be one or more of: "FWZ", "ISAKMP" (meaning IKE).

"X" in OID	fw1person	fw1template	default
28	y	y	"FWZ"

fw1userPwdPolicy

Defines when and by whom the password should and can be changed.

"X" in OID	fw1person
29	y

fw1badPwdCount

Number of allowed wrong passwords entered sequentially.

"X" in OID	fw1person
30	y

fw1lastLoginFailure

Time of the last login failure.

"X" in OID	fw1person
31	4

memberof template

DN of the template that the user is a member of.

"X" in OID	fw1person
33	4

Netscape LDAP Schema

To add the propriety schema to your Netscape directory server, use the file `schema.ldif` in the `$FWDIR/lib/ldap` directory.

Important - This deletes the objectclass definition from the schema and adds the updated one in its place.

We recommend that you back up the User Directory server before you run the command.

The `ldif` file:

- Adds the new attributes to the schema
- Deletes old definitions of `fw1person` and `fw1template`
- Adds new definitions of `fw1person` and `fw1template`

To change the Netscape LDAP schema, run the **ldapmodify** command with the **schema.ldif** file.

On some server versions, the `delete objectclass` operation can return an error, even if it was successful. Use `ldapmodify` with the `-c` (continuous) option.

User Directory Profiles

The User Directory profile is a configurable LDAP policy that lets you define more exact User Directory requests and enhances communication with the server. Profiles control most of the LDAP server-specific knowledge. You can manage diverse technical solutions, to integrate LDAP servers from different vendors.

Use User Directory profiles to make sure that the user management attributes of a Security Management Server are correct for its associated LDAP server. For example, if you have a certified OPSEC User Directory server, apply the OPSEC_DS profile to get enhanced OPSEC-specific attributes.

LDAP servers have difference object repositories, schemas, and object relations.

- The organization's user database may have unconventional object types and relations because of a specific application.

- Some applications use the `cn` attribute in the User object's Relatively Distinguished Name (RDN) while others use `uid`.
- In Microsoft Active Directory, the user attribute `memberOf` describes which group the user belongs to, while standard LDAP methods define the `member` attribute in the group object itself.
- Different servers implement different storage formats for passwords.
- Some servers are considered v3 but do not implement all v3 specifications. These servers cannot extend the schema.
- Some LDAP servers already have built in support for certain user data, while others require a Check Point schema extended attribute. For example, Microsoft Active Directory has the `accountExpires` user attribute, but other servers require the Check Point attribute `fw1expirationdate`, which is part of the Check Point defined `fw1person` objectclass.
- Some servers allow queries with non-defined types, while others do not.

Default User Directory Profiles

These profiles are defined by default:

- **OPSEC_DS** - the default profile for a standard OPSEC certified User Directory.
- **Netscape_DS** - the profile for a Netscape Directory Server.
- **Novell_DS** - the profile for a Novell Directory Server.
- **Microsoft_AD** - the profile for Microsoft Active Directory.

Modifying User Directory Profiles

Profiles have these major categories:

- **Common** - Profile settings for reading and writing to the User Directory.
- **Read** - Profile settings only for reading from the User Directory.
- **Write** - Profile settings only for writing to the User Directory.

Some of these categories list the same entry with different values, to let the server behave according to type of operation. You can change certain parameters of the default profiles for finer granularity and performance tuning.

To apply a profile:

1. Open the Account Unit.
2. Select the profile.

To change a profile:

1. Create a new profile.
2. Copy the settings of a User Directory profile into the new profile.
3. Change the values.

Fetch User Information Effectively

User Directory servers organize groups and members through different means and relations. User Directory operations are performed by Check Point on users, groups of users, and user templates where the template is defined as a group entry and users are its members. The mode in

which groups/templates and users are defined has a profound effect on the performance of some of the Check Point functionality when fetching user information. There are three different modes:

- Defining a "Member" attribute per member, or "*Member*" user-to-group membership mode. In this case, each member of a specific group gets the 'Member" attribute, where the value of this attribute is the DN of that member.
- Defining a "Memberof" attribute per group, or "*MemberOf*" user-to-group membership mode. In this case, each group gets the "Memberof" attribute per group, where the value of this attribute is the DN of a group entry. This is referred to as "*MemberOf*" user-to-group membership mode.
- Defining a "Memberof" attribute per member and group, or "*Both*" user-to-group membership mode. In this case both members and groups are given the "Memberof" attribute.

The most effective mode is the "MemberOf" and "Both" modes where users' group membership information is available on the user itself and no additional User Directory queries are necessary.

Setting User-to-Group Membership Mode

Set the user-to-group membership mode in the profile objects for each User Directory server in `objects_5_0.C`.

- To specify the user-to-group and template-to-group membership mode set the `GroupMembership` attribute to one of the following values: Member, MemberOf, Both accordingly.
- To specify the user-to-template membership mode set the `TemplateMembership` attribute to one of the following values: Member, MemberOf accordingly.

After successfully converting the database, set the User Directory server profile in `objects_5_0.C` to the proper membership setting and start the Security Management server. Make sure to install policy/user database on all gateways to enable the new configuration.

Profile Attributes

Attributes:

UserLoginAttr

The unique username User Directory attribute (uid). In addition, when fetching users by the username, this attribute is used for query.

default	Other
• uid (most servers) • SamAccountName (in Microsoft_AD)	One value allowed

UserPasswordAttr

This user password User Directory attribute.

default	Other
• userPassword (most servers) • unicodePwd (in Microsoft_AD)	One value allowed

TemplateObjectClass

The object class for Check Point User Directory templates. If you change the default value with another objectclass, make sure to extend that objectclass schema definition with relevant attributes from `fw1template`.

default	Other
fw1template	Multiple values allowed

ExpirationDateAttr

The account expiration date User Directory attribute. This could be a Check Point extended attribute or an existing attribute.

default	Other
• fw1expiration-date (most servers) • accountExpires (in Microsoft_AD)	One value allowed

ExpirationDateFormat

Expiration date format. This format will be applied to the value defined at `ExpirationDateAttr`.

default	Other
CP format is yyyymmdd	One value allowed

PsswdDateFormat

The format of the password modified date User Directory attribute. This formation will be applied to the value defined at `PsswdDateAttr.`

default	Other
• CP (most servers) format is yyyymmdd • MS (in Microsoft_AD)	One value allowed

PsswdDateAttr

The password last modified date User Directory attribute.

default	Other
• fw1pwdLastMod (most servers) • pwdLastSet (in Microsoft_AD)	One value allowed

BadPwdCountAttr

User Directory attribute to store and read bad password authentication count.

default	Other
fw1BadPwdCount	One value allowed

ClientSideCrypt

If 0, the sent password will not be encrypted. If 1, the sent password will be encrypted with the algorithm specified in the DefaultCryptAlgorithm.

default	Other
• 0 for most servers • 1 for Netscape_DS if not using encrypted password, SSL is recommended	One value allowed

DefaultCryptAlgorith

The algorithm used to encrypt a password before updating the User Directory server with a new password.

default	Other
• Plain (for most servers) • Crypt (for Netscape_DS) • SHAI1	One value allowed

CryptedPasswordPrefix

The text to prefix to the encrypted password when updating the User Directory server with a modified password.

default	Other
{Crypt} (for Netscape_DS)	One value allowed

PhoneNumberAttr

User Directory attribute to store and read the user phone number.

default	Other
internationalisednumber	One value allowed

AttributesTranslationMap

General purpose attribute translation map, to resolve problems related to peculiarities of different server types. For example, an X.500 server does not allow the "-" character in an attribute name. To enable the Check Point attributes containing "-", specify a translation entry: (e.g., "`fw1-expiration =fw1expiration`").

default	Other
none	Multiple values allowed

ListOfAttrsToAvoid

All attribute names listed here will be removed from the default list of attributes included in read/write operations. This is most useful in cases where these attributes are not supported by the User Directory server schema, which might fail the entire operation. This is especially relevant when the User Directory server schema is not extended with the Check Point schema extension.

Default	Other
There are no values by default. In case the User Directory server was not extended by the Check Point schema, the best thing to do is to list here all the new Check Point schema attributes.	Multiple values allowed

BranchObjectClass

Use this attribute to define which type of objects (objectclass) is queried when the object tree branches are displayed after the Account Unit is opened in SmartConsole.

Default	Other
• Organization OrganizationalUnit Domain (most servers) • Container (extra for Microsoft_AD)	Multiple values allowed

BranchOCOperator

If One is set, an ORed query will be sent and every object that matches the criteria will be displayed as a branch. If All, an ANDed query will be sent and only objects of all types will be displayed.

Default	Other
One	One value allowed

OrganizationObjectClass

This attribute defines what objects should be displayed with an organization object icon. A new object type specified here should also be in BranchObjectClass.

Default	Other
organization	Multiple values allowed

OrgUnitObjectClass

This attribute defines what objects should be displayed with an organization object icon. A new object type specified here should also be in BranchObjectClass.

Default	Other
• organizationalUnit (most servers) • Contained (added to Microsoft_AD)	Multiple values allowed

DomainObjectClass

This attribute defines what objects should be displayed with a Domain object icon. A new object type specified here should also be in BranchObjectClass.

Default	Other
Domain	Multiple values allowed

UserObjectClass

This attribute defines what objects should be read as user objects. The user icon will be displayed on the tree for object types specified here.

Default	Other
• User (in Microsoft_AD) • Person OrganizationalPerson InertOrgPerson FW1 Person (most servers)	Multiple values allowed

UserOCOperator

If 'one' is set, an ORed query will be sent and every object that matches one of the types will be displayed as a user. If 'all' and ANDed query will be sent and only objects of all types will be displayed.

Default	Other
One	One value allowed

GroupObjectClass

This attribute defines what objects should be read as groups. The group icon will be displayed on the tree for objects of types specified here.

Default	Other
Groupofnames Groupofuniquenames (most servers) Group Groupofnames (in Microsoft_AD)	Multiple values allowed

GroupOCOperator

If 'one' is set an ORed query will be sent and every object that matches one of the types will be displayed as a user. If 'all' an ANDed query will be sent and only objects of all types will be displayed.
GroupMembership

Default	Other
One	One value allowed

Defines the relationship Mode between the group and its members (user or template objects) when reading group membership.

Default	Other
• Member mode defines the member DN in the Group object (most servers) • MemberOf mode defines the group DN in the member object (in Microsoft_AD) • Modes define member DN in Group object and group DN in Member object.	One value allowed

UserMembershipAttr

Defines what User Directory attribute to use when reading group membership from the user or template object if GroupMembership mode is 'MemberOf' or 'Both' you may be required to extend the user/template object schema in order to use this attribute.

Default	Other
MemberOf	One value allowed

TemplateMembership

Defines the user to template membership mode when reading user template membership information.

Default	Other
• Member mode defines the member DN in the Group object (most servers) • MemberOf mode defines the group DN in the member object (in Microsoft_AD)	One value allowed

TemplateMembershipAttr

Defines which attribute to use when reading the User members from the template object, as User DNs, if the TemplateMembership mode is Member.

Default	Other
member	Multiple values allowed

UserTemplateMembershipAttr

Defines which attribute to use when reading from the User object the template DN associated with the user, if the TemplateMembership mode is MemberOf.

Default	Other
member	Multiple values allowed

OrganizationRDN

This value will be used as the attribute name in the Relatively Distinguished Name (RDN) when you create a new organizational unit in SmartConsole.

Default	Other
o	One value allowed

OrgUnitRDN

This value is used as the attribute name in the Relatively Distinguished Name (RDN) when you create a new organizational Unit in SmartConsole.

Default	Other
ou	One value allowed

UserRDN

This value is used as the attribute name in the Relatively Distinguished Name (RDN), when you create a new User object in SmartConsole.

Default	Other
cn	One value allowed

GroupRDN

This value is used as the attribute name for the RDN, when you create a new Group object in SmartConsole.

Default	Other
cn	One value allowed

DomainRDN

This value is used as the attribute name for the RDN, when you create a new Domain object in SmartConsole.

Default	Other
dc	One value allowed

AutomaticAttrs

This field is relevant when you create objects in SmartConsole. The format of this field is `Objectclass:name:value` meaning that if the object created is of type `ObjectClass` then additional attributes will be included in the created object with name '`name`' and value '`value`'.

Default	Other
user:userAccountControl:66048 For Microsoft_AD This means that when a user object is created an extra attribute is included automatically: userAccountControl with the value 66048	Multiple values allowed

GroupObjectClass

This field is used when you modify a group in SmartConsole. The format of this field is **ObjectClass:memberattr** meaning that for each group objectclass there is a group membership attribute mapping. List here all the possible mappings for this User Directory server profile. When a group is modified, based on the group's objectclass the right group membership mapping is used.

Default	Other
groupOfNames:member groupOfUniqueNames:uniqueMember (All other servers)	Multiple values allowed

OrgUnitObjectClass

This determines which ObjectClass to use when creating/modifying an OrganizationalUnit object. These values can be different from the read counterpart.

Default	Other
OrganizationalUnit	Multiple values allowed

OrganizationObjectClass

This determines which ObjectClass to use when creating and/or modifying an Organization object. These values can be different from the read counterpart.

Default	Other
Organization	Multiple values allowed

UserObjectClass

This determines which ObjectClass to use when creating and/or modifying a user object. These values can be different from the read counterpart.

Default	Other
User (in Microsoft_AD) person organizationalPerson inetOrgPerson fw1Person (All other servers)	Multiple values allowed

DomainObjectClass

Determines which ObjectClass to use when creating and/or modifying a domain context object. These values can be different from the read counterpart.

Default	Other
Domain	Multiple values allowed

Microsoft Active Directory

The Microsoft Windows 2000 advanced server (or later) includes a sophisticated User Directory server that can be adjusted to work as a user database for the Security Management server.

By default, the Active Directory services are disabled. In order to enable the directory services:

- run the `dcpromo` command from the **Start > Run** menu, *or*
- run the Active Directory setup wizard using the **System Configuration** window.

The Active Directory has the following structure:

```
DC=qa, DC=checkpoint,DC=com
CN=Configuration,DCROOT
CN=Schema,CN=Configuration,DCROOT
CN=System,DCROOT
CN=Users,DCROOT
```

```
CN=Builtin,DCROOT
CN=Computers,DCOOT
OU=Domain Controllers,DCROOT
...
```

Most of the user objects and group objects created by Windows 2000 tools are stored under the `CN=Users, DCROOT` branch, others under `CN=Builtin, DCROOT` branch, but these objects can be created under other branches as well.

The branch `CN=Schema, CN=Configuration, DCROOT` contains all schema definitions.

Check Point can take advantage of an existing Active Directory object as well as add new types. For users, the existing user can be used "as is" or be extended with fw1person as an auxiliary of "User" for full feature granularity. The existing Active Directory "Group" type is supported "as is". A User Directory template can be created by adding the fw1template objectclass. This information is downloaded to the directory using the `schema_microsoft_ad.ldif` file (see Adding New Attributes to the Active Directory (on page 239)).

Performance

The number of queries performed on the directory server is significantly low with Active Directory. This is achieved by having a different object relations model. The Active Directory group-related information is stored inside the user object. Therefore, when fetching the user object no additional query is necessary to assign the user with the group. The same is true for users and templates.

Manageability

SmartConsole allows the creation and management of existing and new objects. However, some specific Active Directory fields are not enabled in SmartConsole.

Enforcement

It is possible to work with the existing Active Directory objects without extending the schema. This is made possible by defining an Internal Template object and assigning it with the User Directory Account Unit defined on the Active Directory server.

For example, if you wish to enable all users with IKE+Hybrid based on the Active Directory passwords, create a new template with the IKE properties enabled and "Check Point password" as the authentication method.

Updating the Registry Settings

To modify the Active Directory schema, add a new registry DWORD key named `Schema Update Allowed` with the value different from zero under `HKLM\System\CurrentControlSet\Services\NTDS\Parameters`.

Delegating Control

Delegating control over the directory to a specific user or group is important since by default the Administrator is not allowed to modify the schema or even manage directory objects through User Directory protocol.

To delegate control over the directory:

1. Display the **Users and Computers Control** console.
2. Right-click on the domain name displayed in the left pane and choose **Delegate control** from the right-click menu.

   The Delegation of Control wizard window is displayed.
3. Add an Administrator or another user from the System Administrators group to the list of users who can control the directory.
4. Reboot the machine.

Extending the Active Directory Schema

Modify the file with the Active Directory schema, to use SmartConsole to configure the Active Directory users.

To extend the Active Directory schema:

1. From the Security Gateway, go to the directory of the schema file: `$FWDIR/lib/ldap`.
2. Copy `schmea_microsoft_ad.ldif` to the **C:** drive in the Active Directory server.
3. From Active Directory server, with a text editor open the schema file.
4. Find the value `DOMAINNAME`, and replace it with the name of your domain in LDIF format.

   For example, the domain `sample.checkpoint.com` in LDIF format is: `DC=sample,DC=checkpoint,DC=com`
5. Make sure that there is a dash character `-` at the end of the `modify` section.

   This is an example of the `modify` section.

```
dn: CN=User,CN-Schema,CN=Configuration,DC=sample,DC=checkpoint,DC=com
changetype: modify
add: auxiliaryClass
auxiliaryClass: 1.3.114.7.3.2.0.2
-
```

6. Run `ldifde -i -f c:/schema_microsoft_ad.ldif`

Adding New Attributes to the Active Directory

Below is the example in LDAP Data Interchange (LDIF) format that adds one attribute to the Microsoft Active Directory:

```
dn:CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
changetype: add
   adminDisplayName: fw1auth-method
   attributeID: 1.3.114.7.4.2.0.1
   attributeSyntax: 2.5.5.4
   cn: fw1auth-method
   distinguishedName:
   CN=fw1auth-method,CN=Schema,CN=Configuration,DCROOT
   instanceType: 4
   isSingleValued: FALSE
   LDAPDisplayName: fw1auth-method
   name: fw1auth-method
   objectCategory:
   CN=Attribute-Schema,CN=ConfigurationCN=Schema,CN=Configuration,DCROOT
```

```
ObjectClass: attributeSchema
oMSyntax: 20
rangeLower: 1
rangeUpper: 256
showInAdvancedViewOnly: TRUE
```

All Check Point attributes can be added in the same way.

The definitions of all attributes in LDIF format are contained in the `schema_microsoft_ad.ldif` file located in the `$FWDIR/lib/ldap` directory.

Before attempting to run the `ldapmodify` command, edit `schema_microsoft_ad.ldif` and replace all instances of `DCROOT` with the domain root of your organization. For example if your domain is `support.checkpoint.com`, replace `DCROOT` with `dc=support,dc=checkpoint,dc=com`.

After modifying the file, run the `ldapmodify` command to load the file into the directory. For example if you use the Administrator account of the `dc=support,dc=checkpoint,dc=com domain` the command syntax will be as follows:

Note - A shell script is available for UNIX gateways. The script is at: `$FWDIR/lib/ldap/update_schema_microsoft_ad`

```
 ldapmodify -c -h support.checkpoint.com -D
cn=administrator,cn=users,dc=support,dc=checkpoint,dc=com" -w SeCrEt -f
$FWDIR/lib/ldap/schema_microsoft_ad.ldif
```

Retrieving Information from a User Directory Server

When a gateway requires user information for authentication, it goes through this process:

1. The gateway searches for the user in the *internal users database*.
2. If the specified user is not defined in the *internal users database*, the gateway queries the *LDAP server* defined in the Account Unit with the highest priority.
3. If the query against an LDAP server with the highest priority fails (for example, the connection is lost), the gateway queries the server with the next highest priority.

   If there is more than one Account Unit, the Account Units are queried concurrently. The results of the query are taken from the first Account Unit to meet the conditions, or from all the Account Units which meet the conditions.
4. If the query against all LDAP servers fails, the gateway matches the user against the generic external user profile.

Running User Directory Queries

Use queries to get User Directory user or group data. For best performance, query Account Units when there are open connections. Some connections are kept open by the gateways, to make sure the user belongs to a group that is permitted to do a specified operation.

To query User Directory:

1. In SmartConsole, go to **Manage & Settings** > **Blades**.
2. Click **Configure in SmartDashboard**.

   SmartDashboard opens.
3. In the **Objects Tree**, click **Users**.
4. Double-click the **Account Unit** to open a connection to the LDAP server.
5. Right-click the **Account Unit** and select **Query Users/Group**.

The **LDAP Query Search** window opens.

Click **Advanced** to select specified objects types, such as Users, groups, or templates.

6. Define the query.
7. To add more conditions, select or enter the values and click **Add**.

Query conditions:

- **Attributes** - Select a user attribute from the drop-down list, or enter an attribute.
- **Operators** - Select an operator from the drop-down list.
- **Value** - Enter a value to compare to the entry's attribute. Use the same type and format as the actual user attribute. For example, if **Attribute** is fw1expiration-date, then **Value** must be in the **yyyymmdd** syntax.
- **Free Form** - Enter your own query expression. See RFC 1558 for information about the syntax of User Directory (LDAP) query expressions.
- **Add** - Appends the condition to the query (in the text box to the right of **Search Method**).

Example of a Query

If you create a query where:

- **Attributes** = **mail**
- **Contains**
- **Value** = **Andy**

The server queries the User Directory with this filter:

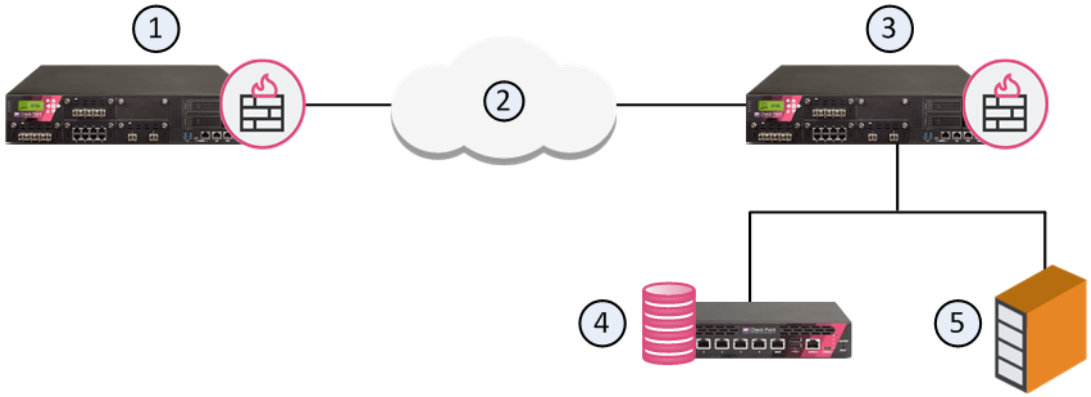
```
filter:(&(|(objectclass=fw1person)(objectclass=person)
(objectclass=organizationalPerson)(objectclass=inetOrgPerson))
(|(cn=Brad)(mail=*Andy*)))
```

Querying Multiple LDAP Servers

The Security Management server and the gateways can work with multiple LDAP servers concurrently. For example, if a gateway needs to find user information, and it does not know where the specified user is defined, it queries all the LDAP servers in the system. (Sometimes a gateway can find the location of a user by looking at the user DN, when working with certificates.)

Deploying User Directory

User Directory integrates the Security Management Server and an LDAP server and lets the Security Gateways use the LDAP information.



Item	Description
1	Security Gateway - Retrieves LDAP user information and CRLs
2	Internet
3	Security Gateway - Queries LDAP user information, retrieves CRLs, and does bind operations for authentication
4	Security Management Server - Uses User Directory to manage user information
5	LDAP server - Server that holds one or more Account Units

Enabling User Directory

In SmartConsole, enable the Security Management Server to manage users in the Account Unit ("Working with LDAP Account Units" on page 243).

Note - You cannot use the SmartConsole User Database when the User Directory LDAP server is enabled.

To enable User Directory on the Security Management Server:

1. From the Menu, select **Global Properties** > **User Directory**.
   The **User Directory** page opens.
2. Select **Use User Directory for Security Gateways**.
3. Configure login and password settings.
4. Click **OK**.
5. In the **Gateways & Servers** view (Ctrl+1), open the Security Management Server object for editing
6. On **General Properties** page, **Management** tab, select **Network Policy Management** and **User Directory**.
7. Click **OK**.
8. Install the policy.

Account Units

An *Account Unit* represents branches of user information on one or more LDAP servers. The Account Unit is the interface between the LDAP servers and the Security Management Server and Security Gateways.

You can have a number of Account Units representing one or more LDAP servers. Users are divided among the branches of one Account Unit, or between different Account Units.

Note - When you enable the Identity Awareness and Mobile Access Software Blades, SmartConsole opens a First Time Configuration Wizard. The **Active Directory Integration** window of this wizard lets you create a new AD Account Unit. After you complete the wizard, SmartConsole creates the AD object and Account Unit.

Working with LDAP Account Units

Use the **LDAP Account Unit Properties** window in SmartConsole to edit an existing Account Unit or to create a new one manually.

To edit an existing LDAP Account Unit:

1. In SmartConsole, open the **Object Explorer** (Ctrl+E).
2. Select **Servers** > **LDAP Account Units**.
3. Right-click the LDAP Account Unit and select **Edit**.
   The **LDAP Account Unit Properties** window opens.
4. Edit the settings in these tabs:
   - **General** ("General Tab" on page 244) - Configure how the Security Management Server uses the Account Unit
   - **Servers** ("Configuring an LDAP Server" on page 244) - Manage LDAP servers that are used by this Account Unit
   - **Objects Management** ("Objects Management Tab" on page 245) - Configure the LDAP server for the Security Management Server to query and the branches to use
   - **Authentication** ("Authentication Tab" on page 245) - Configure the authentication scheme for the Account Unit
5. Click **OK**.
6. Install the policy.

To create a new LDAP Account Unit:

1. In the **Objects** tab, click **New > More > Server > LDAP Account unit**.
   The **LDAP Account Unit Properties** window opens.
2. Configure the settings on these tabs:
   - **General** ("General Tab" on page 244) - Configure how the Security Management Server uses the Account Unit
   - **Servers** ("Configuring an LDAP Server" on page 244) - Manage LDAP servers that are used by this Account Unit
   - **Objects Management** ("Objects Management Tab" on page 245) - Configure the LDAP server for the Security Management Server to query and the branches to use
   - **Authentication** ("Authentication Tab" on page 245) - Configure the authentication scheme for the Account Unit
3. Click **OK**.

4. Install the policy.

General Tab

These are the configuration fields in the **General** tab:

- **Name** - Name for the Account Unit
- **Comment** - Optional comment
- **Color** - Optional color associated with the Account Unit
- **Profile** - LDAP vendor
- **Domain** - Domain of the Active Directory servers, when the same user name is used in multiple Account Units (this value is also necessary for AD Query and SSO)
- **Prefix** - Prefix for non-Active Directory servers, when the same user name is used in multiple Account Units
- **Account Unit usage** - Select applicable options:
  - **CRL retrieval** - The Security Management Server manages how the CA sends information about revoked licenses to the Security Gateways
  - **User Management** - The Security Management Server uses the user information from this LDAP server (User Directory must be enabled on the Security Management Server)

    Note - LDAP SSO (Single Sign On) is only supported for Account Unit objects that use **User Management**.
  - **Active Directory Query** - This Active Directory server is used as an Identity Awareness source.

    Note - This option is only available if the **Profile** is set to **Microsoft_AD**.
- **Enable Unicode support** - Encoding for LDAP user information in non-English languages
- **Active Directory SSO configuration** - Click to configure Kerberos SSO for Active Directory - **Domain Name**, **Account Name**, **Password**, and **Ticket encryption method**

Configuring an LDAP Server

You can add, edit, or delete LDAP server objects.

To configure an LDAP server for the Account Unit:

1. To add a new server, click **Add**. To edit an existing one, select it from the table and click **Edit**.
   The **LDAP Server Properties** window opens.
2. From the **Host** drop-down menu, select the server object.
   If necessary, create a new SmartConsole server object:
   a) Click **New**.
   b) In the **New Host** window opens, enter the settings for the LDAP server.
   c) Click **OK**.
3. Enter the login credentials and the **Default priority**.
4. Select access permissions for the Check Point Gateways:
   - **Read data from this server**
   - **Write data to this server**
5. In the **Encryption** tab, configure the optional SSL encryption settings. To learn about these settings, see the Help. Click **?** or press F1 in the **Encryption** tab.

6. Click **OK**.

To remove an LDAP server from the Account Unit:

1. Select a server from the table.
2. Click **Remove**.

If all the configured servers use the same login credentials, you can modify those simultaneously.

To configure the login credentials for all the servers simultaneously:

1. Click **Update Account Credentials**.
   The **Update Account to All Servers** window opens.
2. Enter the login credentials.
3. Click **OK**.

Objects Management Tab

Configure the LDAP server for the Security Management Server to query and the branches to fetch.

Note - Make sure there is LDAP connectivity between the Security Management Server and the LDAP Server that holds the management directory.

To configure LDAP query parameters:

1. From the **Manage objects on** drop-down menu, select the LDAP server object.
2. Click **Fetch branches**.
   The Security Management Server queries and shows the LDAP branches.
3. Configure **Branches in use**:
   - To add a branch, click **Add** and in the LDAP Branch Definition window that opens, enter a new **Branch Path**
   - To edit a branch, click **Edit** and in the LDAP Branch Definition window that opens, modify the **Branch Path**
   - To delete a branch, select it and click **Delete**
4. Select **Prompt for password when opening this Account Unit**, if necessary (optional).
5. Configure the number of **Return entries** that are stored in the LDAP database (the default is 500).

Authentication Tab

These are the configuration fields in the Authentication tab:

- **Use common group path for queries** - Select to use one path for all the LDAP group objects (only one query is necessary for the group objects)
- **Allowed authentication schemes** - Select one or more authentication schemes allowed to authenticate users in this Account Unit - **Check Point Password**, **SecurID**, **RADIUS**, **OS Password**, or **TACACS**
- Users' default values - The default settings for new LDAP users:
  - **User template** - Template that you created
  - **Default authentication scheme** - one of the authentication schemes selected in the **Allowed authentication schemes** section

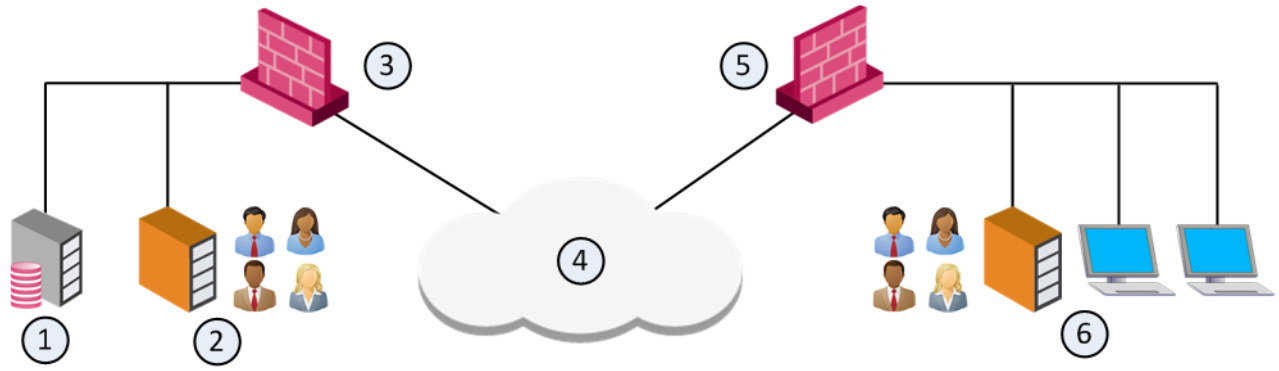
- **Limit login failures** (optional):
  - **Lock user's account after** - Number of **login failures**, after which the account gets locked
  - **Unlock user's account after** - Number of **seconds**, after which the locked account becomes unlocked
- **IKE pre-shared secret encryption key** - Pre-shared secret key for IKE users in this Account Unit

Modifying the LDAP Server

1. On the **LDAP Account Unit Properties > Servers** tab, double-click a server.
   The **LDAP Server Properties** window opens.
2. On the **General** tab, you can change:
   - Port of the LDAP server
   - Login DN
   - Password
   - Priority of the LDAP server, if there are multiple servers
   - Security Gateway permissions on the LDAP server
3. On the **Encryption** tab, you can change the encryption settings between Security Management Server / Security Gateways and LDAP server.
   If the connections are encrypted, enter the encryption port and strength settings.
   Note - User Directory connections can be authenticated by client certificates from a Certificate Authority (CA) ("Authenticating with Certificates" on page 247). To use certificates, the LDAP server must be configured with SSL strong authentication.

Account Units and High Availability

With User Directory replications for High Availability, one Account Unit represents all the replicated User Directory servers. For example, two User Directory server replications can be defined on one Account Unit, and two Security Gateways can use the same Account unit.



Item	Description
1	**Security Management Server**. Manages user data in User Directory. It has an Account Unit object, where the two servers are defined.
2	**User Directory server** replication.
3	**Security Gateway**. Queries user data and retrieves CRLs from nearest User Directory server replication (2).

Item	Description
4	Internet
5	**Security Gateway**. Queries user data and retrieves CRLs from nearest User Directory server replication (6).
6	**User Directory server** replication.

Setting High Availability Priority

With multiple replications, define the priority of each LDAP server in the Account Unit. Then you can define a server list on the Security Gateways.

Select one LDAP server for the Security Management server to connect to. The Security Management server can work with one LDAP server replication. All other replications must be synchronized for standby.

To set priority on the Account Unit:

1. Open the **LDAP Account Unit Properties** window.
2. Open the **Servers** tab.
3. Add the LDAP servers of this Account Unit in the order of the priority that you want.

Authenticating with Certificates

The Security Management Server and Security Gateways can use certificates to secure communication with LDAP servers. If you do not configure certificates, the management server, Security Gateways, and LDAP servers communicate without authentication.

To configure User Directory to use certificates:

1. On each Account Unit, to which you want to authenticate with a certificate, set the `ldap_use_cert_auth` attribute to `true`:
   a) Connect with GuiDBedit Tool (see sk13009 http://supportcontent.checkpoint.com/solutions?id=sk13009) to Security Management Server.
   b) In the left pane, browse to **Table > Managed Objects > servers**.
   c) In the right pane, select the Account Unit object.
   d) In the bottom pane, search for the `ldap_use_cert_auth` attribute, and set it to **true**.
   e) Save the changes and close GuiDBedit.
2. Log in to SmartConsole.
3. Add a CA object:
   a) From the **Objects Bar** (F11), click **New** > **More** > **Server** > **More** > **Trusted CA**.

      The Certificate Authority Properties window opens.
   b) In Certificate Authority Type, select **External Check Point CA**.
   c) Set the other options of the CA.

4. For all necessary network objects (such as Security Management Server, Security Gateway, Policy Server) that require certificate-based User Directory connections:

   a) On the **IPSec VPN** page of the network object properties, click **Add** in the **Repository of Certificates Available** list.

   Note - a management-only server does not have an IPSec VPN page. The User Directory on a management-only server cannot be configured to authenticate to an LDAP server using certificates.

   b) In the **Certificate Properties** window, select the defined CA.

5. Test connectivity between the Security Management Server and the LDAP Server ("Managing LDAP Information" on page 248).

Managing Users on a User Directory Server

In SmartConsole, users and user groups in the Account Unit show in the same tree structure as on the LDAP server.

- To see User Directory users, open **Users and Administrators**. The **LDAP Groups** folder holds the structure and accounts of the server.
- You can change the User Directory templates. Users associated with this template get the changes immediately. If you change user definitions manually in SmartConsole, the changes are immediate on the server.

Distributing Users in Multiple Servers

The users of an organization can be distributed across several LDAP servers. Each LDAP server must be represented by a separate Account Unit.

Managing LDAP Information

User Directory lets you use SmartDashboard to manage information about users and OUs (Organizational Units) that are stored on the LDAP server.

To manage LDAP information from SmartDashboard:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. Click **Configure in SmartDashboard**.

   SmartDashboard opens.
3. From the object tree, select **Servers and OPSEC**.
4. Double-click the Account Unit.

   The LDAP domain is shown.
5. Double-click the LDAP branch.

   The Security Management Server queries the LDAP server and SmartDashboard shows the LDAP objects.
6. Expand the **Objects List** pane.
7. Double-click the LDAP object.

   The **Objects List** pane shows the user information.
8. Right-click a user and select **Edit**.

   The **LDAP User Properties** window opens.
9. Edit the user information and settings and then click **OK**.

LDAP Groups for the User Directory

Create LDAP groups for the User Directory. These groups classify users according to type and can be used in Policy rules. You can add users to groups, or you can create dynamic filters.

To create LDAP groups for User Directory:

1. In SmartConsole, open **Object Categories > New > More > Users > LDAP group**.
2. In the **New LDAP Group** window that opens, select the **Account Unit** for the User Directory group.
3. Define **Group's Scope** - select one of these:
   - **All Account-Unit's Users** - All users in the group
   - **Only Sub Tree** - Users in the specified branch
   - **Only Group in branch** - Users in the branch with the specified DN prefix
4. Apply an advanced **LDAP filter:**
   a) Click **Apply filter for dynamic group**.
   b) Enter the filter criteria.
5. Click **OK**.

Examples

- If the User objects for managers in your organization have the object class "myOrgManager", define the Managers group with the filter: **objectclass=myOrgManagers**
- If users in your organization have an e-mail address ending with us.org.com, you can define the US group with the filter: **mail=*us.org.com**

Access Roles

Access role objects let you configure network access according to:

- Networks
- Users and user groups
- Computers and computer groups
- Remote access clients - will be supported with R80.x gateways

After you activate the Identity Awareness Software Blade, you can create access role objects and use them in the **Source** and **Destination** columns of Access Control Policy rules.

Adding Access Roles

Important: Before you add Active Directory users, machines, or groups to an access role, make sure there is LDAP connectivity between the Security Management Server and the AD Server that holds the management directory. The management directory is defined on the **Objects Management** tab in the **Properties** window of the **LDAP Account Unit**.

To create an access role:

1. In the object tree, click **New> More > Users > Access Role**.
   The **New Access Role** window opens.
2. Enter a **Name** for the access role.

3. Enter a **Comment** (optional).
4. Select a **Color** for the object (optional).
5. In the **Networks** pane, select one of these:
   - **Any network**
   - **Specific networks** - For each network, click + and select the network from the list
6. In the **Users** pane, select one of these:
   - **Any user**
   - **All identified users** - includes any user identified by a supported authentication method (internal users, Active Directory users, or LDAP users).
   - **Specific users/groups** - For each user or user group, click + and select the user or the group from the list
7. In the **Machines** pane, select one of these:
   - **Any machine**
   - **All identified machines** - includes machines identified by a supported authentication method (Active Directory).
   - **Specific machines** - For each machine, click + and select the machine from the list
8. In the **Remote Access Clients** pane, select the clients for remote access.
9. Click **OK**.

Identity Awareness engine automatically recognizes changes to LDAP group membership and updates identity information, including access roles. For more, see the *R80.10 Identity Awareness Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54825.

Authentication Rules

To make an authentication rule:

1. Add users to user groups.
2. Define an access role ("Access Roles" on page 249) for networks, users and user groups, and computers and computer groups.
3. Make the authentication rules with the access roles in the Source.

Client Certificates for Smartphones and Tablets

In This Section:

To allow your users to access their resources using their handheld devices, make sure they can authenticate to the Gateway with client certificates.

In many organizations, the daily task of assigning and maintaining client certificates is done by a different department than the one that maintains the Security Gateways. The computer help desk, for example. You can create an administrator that is allowed to use SmartConsole to create client certificates, while restricting other permissions ("Giving Permissions for Client Certificates" on page 254).

To configure client certificates, open SmartConsole and go to **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.

To configure the Mobile Access policy, go to **Manage & Settings** > **Blades** > **Mobile Access** > **Configure in SmartDashboard**. The **Client Certificates** page in SmartConsole is a shortcut to the SmartDashboard **Mobile Access** tab, **Client Certificates** page.

Managing Client Certificates

Check Point Mobile Apps for mobile devices can use certificate-only authentication or two-factor authentication with client certificates and username/password. The certificate is signed by the internal CA of the Security Management Server that manages the Mobile Access Security Gateway.

Manage client certificates in **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**..

The page has two panes.

- In the **Client Certificates** pane:
  - Create, edit, and revoke client certificates.
  - See all certificates, their status, expiration date and enrollment key. By default, only the first 50 results show in the certificate list. Click **Show more** to see more results.
  - Search for specified certificates.
  - Send certificate information to users.
- In the **Email Templates for Certificate Distribution** pane:
  - Create and edit email templates for client certificate distribution.
  - Preview email templates.

Creating Client Certificates

Note - If you use LDAP or AD, creation of client certificates does not change the LDAP or AD server. If you get an error message regarding LDAP/AD write access, ignore it and close the window to continue.

To create and distribute certificates with the client certificate wizard:

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. In the **Client Certificates** pane, click **New**.

   The **Certificate Creation and Distribution** wizard opens.
3. In the **Certificate Distribution** page, select how to distribute the enrollment keys to users. You can select one or both options.

   a) **Send an email containing the enrollment keys using the selected email template -** Each user gets an email, based on the template you choose, that contains an enrollment key.

   - **Template** - Select the email template that is used.
   - **Site** - Select the gateway that users connect to.
   - **Mail Server** - Select the mail server that sends the emails.

   You can click **Edit** to view and change its details.

   b) **Generate a file that contains all of the enrollment keys** - Generate a file for your records that contains a list of all users and their enrollment keys.
4. **Optional:** To change the expiration date of the enrollment key, edit the number of days in **Users must enroll within x days**.
5. **Optional:** Add a comment that will show next to the certificate in the certificate list on the **Client Certificates** page.
6. Click **Next**.

   The **Users** page opens.
7. Click **Add** to add the users or groups that require certificates.
   - Type text in the search field to search for a user or group.
   - Select a type of group to narrow your search.
8. When all included users or groups show in the list, click **Generate** to create the certificates and send the emails.
9. If more than 10 certificates are being generated, click **Yes** to confirm that you want to continue.

   A progress window shows. If errors occur, an error report opens.
10. Click **Finish**.
11. Click **Save**.
12. From SmartConsole, install the Policy.

Revoking Certificates

If the status of a certificate is Pending Enrollment, after you revoke it, the certificate does not show in the **Client Certificate** list.

To revoke one or more certificates:

1. Select the certificate or certificates from the **Client Certificate** list.
2. Click **Revoke**.
3. Click **OK**.

After you revoke a certificate, it does not show in the **Client Certificate** list.

Creating Templates for Certificate Distribution

To create or edit an email template:

1. In SmartConsole, select **Security Policies** > **Access Control** > **Access Tools** > **Client Certificates**.
2. To create a new template: In the **Email Templates for Certificate Distribution** pane, select **New.**

   To edit a template: In the **Email Templates for Certificate Distribution** pane, double-click a template.

   The **Email Template** opens.
3. Enter a **Name** for the template.
4. **Optional:** Enter a **Comment**. Comments show in the Mail Template list on the **Client Certificates** page.
5. **Optional:** Click **Languages** to change the language of the email.
6. Enter a **Subject** for the email. Click **Insert Field** to add a predefined field, such as a Username.
7. In the message body add and format text. Click **Insert Field** to add a predefined field, such as Username, Registration Key, or Expiration Date.
8. Click **Insert Link** to add a link or QR code and select the type of link to add.

   For each link type, you select which elements will be added to the mail template:

   - **QR Code** - Users scan the code with their mobile devices.
   - **HTML Link** - Users tap the link on their mobile devices.

     You can select both QR Code and HTML link to include both in the email.

     The text in **Display Text** is the text that shows on the link.

   a. **Certificate and Site Creation** - For users who already have a Check Point app installed. When users scan the CR code or go to the link, it creates the site and registers the certificate.

   - Select the client type that will connect to the site- Select one client type that users will have installed.
     - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
     - **Capsule Connect/VPN** - A full L3 tunnel app that gives users network access to all mobile applications.

   b. **Download Application** - Direct users to download a Check Point App for their mobile devices.

- **Select the client device operating system:**
  - **iOS**
  - **Android**
- **Select the client type to download:**
  - **Capsule Workspace** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
  - **Capsule Connect/VPN -** A full L3 tunnel app that gives users network access to all mobile applications.
- **Select which elements will be added to the mail template:**
  - **QR Code** - Users scan the code with their mobile devices
  - **HTML Link** - Users tap the link on their mobile devices.
  - **Display Text** - Enter the text to show on the HTML link.

9. Click **OK**.
10. **Optional:** Click **Preview in Browser** to see a preview of how the email will look.
11. Click **OK**.
12. Publish the changes

Cloning a Template

Clone an email template to create a template that is similar to one that already exists.

To create a clone of an email template:

1. Select a template from the template list in the **Client Certificates** page.
2. Click **Clone**.
3. A new copy of the selected template opens for you to edit.

Giving Permissions for Client Certificates

You can create an administrator that is allowed to use SmartConsole to create client certificates, and restrict other permissions.

To make an administrator for client certificates:

1. Define an administrator ("Creating and Changing an Administrator Account" on page 26).
2. Create a customized profile for the administrator ("Assigning Permission Profiles to Administrators" on page 29), with permission to handle client certificates. Configure this in the **Others** page of the Administrator Profile. Restrict other permissions.

Preferences and Management Settings

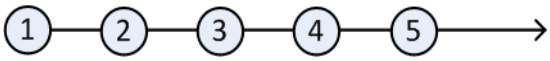
In This Section:

Database Revisions

The Security Management architecture has built-in revisions. Each revision is a new restore point in the database. It contains only the changes from the previous revision. Revisions therefore need only a small amount of disk space, and are created fast. Other benefits of this architecture are:

- Fast policy verification, based on the difference between installed revisions.
- More efficient Management High Availability.
- Safe recovery from a crisis.

This diagram shows the database revisions over time:



1. Install
2. Upgrade
3. Publish
4. Publish
5. Publish

Working with Database Revisions

To see saved database versions:

In SmartConsole, go to **Manage & Settings > Revisions**.

To see the changes made during a specific revision:

1. In the **Manage & Settings > Revisions** window, select revision.
   The bottom pane shows the audit logs of the changes made in the revision.
2. **Optional:** Click **View**.
   A separate read-only SmartConsole session opens.

To delete all versions of the database that are older than the selected version:

1. In the **Manage & Settings > Revisions** window, select a revision.
2. Click **Purge**.

3. In the confirmation window that opens, click **Yes**.

Important - Deletion is irreversible. When you purge, that revision and older revisions are deleted permanently.

Managing a Crisis Using Database Revisions

Case	A connectivity or security problem after making changes to the policy and installing the policy
Solution	1. Go to **Security Policies** > **Installation History**. 2. In the **Policy Installation History**, choose the last known good version and click **Install specific version**. After a Gateway is safely installed, the Gateway has the last good revision, and the Security Management Server has the most recent revision. 3. To see the changes made in the revision, browse the audit logs in the bottom pane of the revision.
Case	Network problem after downloading a Threat Prevention update and installing it on gateways.
Solution	1. From **Security Policies** > **Threat Prevention** > **Threat Tools** > **Updates**, in the **IPS** section, choose an update that is known to be good. 2. Click **Switch to Version**. 3. Install the Threat Prevention Policy. The Gateway gets that version of the IPS protections. Other network objects and policies do not change.

More Database Revision Scenarios:

- Need a full environment restore to a certain point in time.

  Best Practice: Use **Restore Backup**. All work done after the backup is lost. To learn more, see the *R80.20.M1 Gaia Administration Guide*.
  https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_Gaia_AdminGuide/html_frameset.htm
- To revert to a previous state, use **Revert Policy**. This reverts the structure of the Rule Base, but not the objects used in the Rule Base.

Setting IP Address Versions of the Environment

Many objects and rules use IP addresses. Configure the version that your environment uses to see only relevant options.

To set IP address version:

1. Click **Manage & Settings**.
2. Click **Preferences**.
3. Select the IP address version that your environment uses: **IPv4**, **IPv6**, or **IPv4 and IPv6**.
4. Select how you want to see subnets: **Mask Length** or **Subnet Mask**.

Restoring Window Defaults

Some windows in the SmartConsole offer administrators the option to not see the window again. You can undo this selection, and restore all windows to show again.

This option is available only if administrators selected **do not show** in a window.

To restore windows from "do not show":

1. Click **Manage & Settings**.
2. Click **Preferences**.
3. In the **User Preferences** area, click **Restore All Messages**.

Configuring the Login Window

Administrators in your environment use SmartConsole daily. Customize the Login window, to set the environment to comply with your organization's culture.

To customize the Login window:

1. Click **Manage & Settings**.
2. Click **Preferences** > **Login Message**.

   The **Login Message** window opens.
3. Select **Show custom message during login**.
4. In **Customize Message**, enter a **Header** and **Message** for administrators to see.

   The default suggestion is:
   ```
   Warning
   This system is for authorized use only
   ```
5. If you want the message to have a warning icon, in **Customize Layout**, select **Add warning sign**.
6. If you want the Login window to show your organization's logo, in **Customize Layout**, select **Add logo** and then **Browse** to an image file.

Testing New SmartConsole Features

You can influence Check Point product development by selecting and testing one or more of the new features listed here.

To test a new SmartConsole feature:

1. Click **Manage & Settings**.
2. Click **Preferences**.
3. In the **Check Point Lab** area, select the feature you want to test:
   - **Enable Session pane - Review all changes before you publish**

Sync with User Center

You can add information regarding your environment to User Center, such as gateway name, version, and active blades. Check Point uses this additional information for better inventory management, pro-active support, and more efficient ticket resolution.

To learn more, see sk94064 http://supportcontent.checkpoint.com/solutions?id=sk94064.

To sync with User Center:

1. In SmartConsole, click **Manage & Settings**.
2. Click **Sync with User Center**
3. Select **Synchronize information once a day**.

Inspection Settings

You can configure inspection settings for the Firewall:

- Deep packet inspection settings
- Protocol parsing inspection settings
- VoIP packet inspection settings

The Security Management Server comes with two preconfigured inspection profiles for the Firewall:

- **Default Inspection**
- **Recommended Inspection**

When you configure a Security Gateway, the **Default Inspection** profile is enabled for it. You can also assign the **Recommended Inspection** profile to the Security Gateway, or to create a custom profile and assign it to the Security Gateway.

To activate the Inspection Settings, install the Access Control Policy.

Note - In a pre-R80 SmartConsole, Inspection Settings are configured as IPS Protections.

Configuring Inspection Settings

To configure Inspection Settings:

1. In SmartConsole, go to the **Manage & Settings** > **Blades** view.
2. In the **General** section, click **Inspection Settings**.
   The **Inspection Settings** window opens.

You can:

- Edit inspection settings.
- Edit user-defined **Inspection Settings** profiles. You cannot change the **Default Inspection** profile and the **Recommended Inspection** profile.
- Assign **Inspection Settings** profiles to Security Gateways.
- Configure exceptions to settings.

To edit a setting:

1. In the **Inspection Settings** > **General** view, select a setting.
2. Click **Edit**.
3. In the window that opens, select a profile, and click **Edit**.

   The settings window opens.
4. Select the **Main Action:**
   - **Default Action** - preconfigured action
   - **Override with Action** - from the drop-down menu, select an action with which to override the default - **Accept**, **Drop**, **Inactive** (the setting is not activated)
5. Configure the **Logging Settings**

   Select **Capture Packets**, if you want to be able to examine packets that were blocked in Drop rules.
6. Click **OK**.
7. Click **Close**.

To view settings for a certain profile:

1. In the **Inspection Settings** > **General** view, click **View** > **Show Profiles**.
2. In the window that opens, select **Specific Inspection settings profiles**.
3. Select profiles.
4. Click **OK**.

   Only settings for the selected profiles are shown.

You can add, edit, clone, or delete custom Inspection Settings profiles.

To edit a custom Inspection Settings profile:

1. In the **Inspection Settings** > **Profiles** view, select a profile.
2. Click **Delete**, to remove it, or click **Edit** to change the profile name, associated color, or tag.
3. If you edited the profile attributes, click **OK** to save the changes.

To clone an Inspection Settings profile:

1. In the **Inspection Settings** > **Profiles** view, select the profile, and click **Clone**.
2. In the **New Profile** window that opens, edit the profile attributes:
3. Click **OK**.

To add a new Inspection Settings profile:

1. In the **Profiles** view, click **New**.
2. In the **New Profile** window that opens, edit the profile attributes:
3. Click **OK**.

To assign an **Inspection Settings** profile to a Security Gateway:

1. In the **Inspection Settings** > **Gateways** view, select a gateway, and click **Edit**.
2. In the window that opens, select an Inspection Settings profile.
3. Click **OK**.

To configure exceptions to inspection settings:

1. In the **Inspection Settings** > **Exceptions** view, click **New** to add a new exception, or select an exception and click **Edit** to modify an existing one.

   The **Exception Rule** window opens.
2. Configure the exception settings:
   - **Apply To** - select the **Profile** to which to apply the exception
   - **Protection** - select the setting
   - **Source** - select the source **Network Object**, or select **IP Address** and enter a source IP address
   - **Destination** - select the destination **Service Object**
   - **Service** - select **Port/Range**, **TCP** or **UDP**, and enter a destination port number or a range of port numbers
   - **Install On** - select a gateway on which to install the exception
3. Click **OK**.

To enforce the changes, install the Access Control Policy.

Management High Availability

In This Section:

Overview of Management High Availabilty

High Availability is redundancy and database backup for management servers. Synchronized servers have the same policies, rules, user definitions, network objects, and system configuration settings.

Management High Availability uses the built-in revisions technology and allows the High Availability procedure to synchronize only the changes done since the last synchronization. This provides:

- Real-time updates between management peers.
- Minimal effect on the management server resources.

The first management server installed is the primary. If the primary Security Management Server fails, or is off line for maintenance, the administrator can initiate a changeover, so that the secondary server takes over.

Notes:

- High Availability (and Load Sharing) for Security Gateways is covered in the *R80.10 ClusterXL Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54804.
- For Endpoint Security environments, see the *R80.20.M1 Endpoint Security Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_EndpointSecurity_AdminGuide/html_frameset.htm.

The High Availability Environment

A Management High Availability environment includes:

- One Active Security Management Server
- One or more Standby Security Management Server

For full redundancy, the active management server at intervals synchronizes its database with the secondary server or servers.

Active vs. Standby

In a standard High Availability configuration there is one Active server at a time. The administrator uses the Active server manage the High Availability configuration. The Active server automatically synchronizes the standby server(s) at regular intervals. You can open a Standby server only in Read Only mode. If the Active server fails, you can initiate a changeover to make a Standby server become the Active server. If communication with the Active server fails, there may be more than one Active server. This is called Collision Mode.

Primary Server vs. Secondary Server

The sequence in which you install management servers defines them as Primary or Secondary. The first management server installed becomes the Primary active server. When you install more Security Management Servers, you define them as Secondary. Secondary servers are Standby servers by default.

Configuring a Secondary Server in SmartConsole

In the SmartConsole connected to the Primary server, create a network object to show the Secondary Security Management Server. After you publish, synchronize starts between the primary and secondary servers.

To configure the secondary server in SmartConsole:

1. Open SmartConsole.
2. In **Object Categories**, click **New > More > Network Object > Gateways and Servers > Check Point Host**.
3. On the **General Properties** page, enter a unique name and IP address for the server.
4. In the **Software Blades** section, select the **Management** tab.
5. Select **Network Policy Management**.
   This automatically selects the **Secondary Server, Logging and Status**, and **Provisioning**.
6. Create SIC trust between the Secondary Security Management Server and the Primary:
   a) Click **Communication.**
   b) Enter the SIC Activation Key of the secondary server.
   c) Click **Initialize**.
   d) Click **Close**.
7. Click **OK**.
8. Click **Publish** to save these session changes to the database.
   On publish, the initialization and synchronization between the servers starts.
9. Monitor these tasks in the Task List, in the SmartConsole System Information area. Wait for the Task List to show that a full sync has completed.
10. Open the **High Availability Status** window and make sure there is one active server and one standby.

Synchronizing Active and Standby Servers

At intervals, the Active server synchronizes with the standby server or servers, and when you publish the session. Sessions that are not published are not synchronized.

Monitoring High Availability

The **High Availability Status** window shows the status of each Security Management Server in the High Availability configuration.

To see the server status in your High Availability environment:

1. Open SmartConsole and connect to a primary or secondary server.
2. On the **Menu**, click **High Availability**.

The **High Availability Status** window opens.

For the management server and its peer or peers in the High Availability configuration, the **High Availability Status** window shows:

- A Warning or Error message – The message shows if there is a problem between the High Availability peers.
- **Connected To** - The server that SmartConsole is connected to. Also, the High Availability mode of the server (Active or Standby), and the synchronization status and actions of the server ("Monitoring Synchronization Status and Actions" on page 263).
- **Peers** - The servers that the connected server sees. Also, the High Availability mode of each server (Active or Standby), and the synchronization status and actions of each server.

Monitoring Synchronization Status and Actions

Status messages can be general, meaning that they apply to the full system, or they can apply to a specified active or standby server. General messages show in the yellow overview banner.

General Status messages in overview banner	Description
	The database of the primary Security Management Server is identical with the database of the secondary.
Some servers could not be synchronized	A communication issue prevents synchronization, or some other synchronization issue exists.
	The active and standby servers are not communicating.
Communication Problem	Some services are down or cannot be reached.
Collision or HA conflict	More than one management server configured as active. Two active servers cannot sync with each other.

When connected to a specified *active* management server:

Status window area:	Peer Status	Additional Information
Connected to:	Active	SmartConsole is connected to the active management server.

Status window area:	Peer Status	Additional Information
Peers	Standby	The peer is in standby. The message can also show: • Sync problem, last time sync • Synchronized successfully. Last sync time: <time> • No communication
	Not communicating, last sync time	
	Active	A state of collision exists between two servers both defined as active.

When connected to a specified *standby* management server:

Status window area:	Peer Status	Description
Connected to:	Standby	Also shows: last sync time.
Peers	Active	The peer is in standby. The message can also show: • No communication, last sync time • OK., last sync time: <time> • Sync problem, last sync time (in any direction)
	Standby *or* Unknown	Can also show: no communication.

Changeover Between Active and Standby

Changeover between the primary (active) and secondary (standby) management server is not automatic. If the Active fails or it is necessary to change the Active to a Standby, you must do this manually. When the management server becomes Standby it becomes Read Only, and gets all changes from the new Active server.

Changing a Server to Active or Standby

The Active server synchronizes with the standby server or servers at intervals, and when you publish the session. Sessions that are not published are not synchronized.

When the administrator initiates changeover, all public data is synchronized from the new Active to the new Standby server after the Standby becomes Active. Data from the new Active overrides the data on the new Standby. *Unpublished* changes are not synchronized.

Best Practice - We recommend that you publish changes before initiating a changeover to the Standby.

To Interchange the Active and Standby:

1. Open SmartConsole.
2. Connect to the Standby server.
3. On the Menu button, select **High Availability**.
   The **High Availability Status** window opens.
4. Use the **Action** buttons to change the Standby server to Active.

This changes the previous Active server to Standby.

Working in Collision Mode

You can make more than one server Active. You may need to do that if there is no connectivity to the primary. When you change the Standby to Active, it becomes Active without telling the current Active server to become Standby. This is known as *collision mode*. You can later change one of the Active servers to Standby, and return to the standard configuration.

When in collision mode, the Active servers do not sync even if they have network connectivity. When you change one of them to Standby, sync starts and overwrites the data on the Standby server with the remaining Active data.

High Availability Troubleshooting

These error messages show in the **High Availability Status** window when synchronization fails:

Not communicating

Solution:

1. Check connectivity between the servers.
2. Test SIC.

Collision or HA Conflict

More than one management server is configured as active.

Solution:

1. From the main SmartConsole menu, select **Management High Availability**.
   The **High Availability Status** window opens.
2. Use the **Actions** button to set one of the active servers to standby.

Warning - When this server becomes the Standby, all its data is overwritten by the active server.

Sync Error

Solution:

Do a manual sync.

Environments with Endpoint Security

Environments that include Endpoint Security require additional steps and information.

See High Availability in the *R80.20.M1 Endpoint Security Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_EndpointSecurity_AdminGuide/html_frameset.htm for details.

High Availability Disaster Recovery

If the primary management server becomes permanently unavailable:

- Create a new Primary server with the IP address of the original Primary server

  Note - This is not supported for environments with Endpoint Security.

- Promote the Secondary server to Primary and create new licenses.

  IMPORTANT: Check Point product licenses are linked to IP addresses. At the end of the disaster recovery you must make sure that licenses are correctly assigned to your servers.

Promoting a Secondary Server to Primary

The first management server installed is the Primary Server and all servers installed afterwards are Secondary servers. The Primary server acts as the synchronization master. When the Primary server is down, secondary servers cannot synchronize their databases until a Secondary is promoted to Primary and the initial syncs completes.

Note - This is the disaster recovery method supported for High Availability environments with Endpoint Security.

To promote a Secondary server to become the Primary server:

1. On the Secondary Server that you will promote, run:
   ```
   #$FWDIR/bin/promote_util
   #cpstop
   ```
2. Remove the `$FWDIR/conf/mgha*` files. They contain information about the current Secondary settings. These files will be recreated when you start the Check Point services.
3. Make sure you have a `mgmtha` license on the newly promoted server.

   Note - All licenses must have the IP address of the promoted Security Management Server.
4. Run `cpstart` on the promoted server.
5. Open SmartConsole, and:
   a) Make the secondary server active.
   b) Remove all instances of the old Primary Management object. To see all of the instances, right-click the object and select **Where Used**.

      Note - When you remove the old Primary server, all previous licenses are revoked.
   c) Install database.

The ICA Management Tool

The ICA Management Tool lets you:

- Manage certificates
- Run searches
- Recreate CRLs
- Configure the ICA
- Remove expired certificates

Note - The ICA management tool supports TLS.

Check Point ICA is fully compliant with X.509 standards for both certificates and CRLs. See the related X.509 and PKI documentation, and RFC 2459 for more information.

In This Appendix

Using the ICA Management Tool

Use the ICA management tool for user certificate operations only, such as certificate creation. Do not use the ICA management tool to change SIC certificates or VPN certificates. Change SIC and VPN certificates in SmartConsole.

To use the ICA management tool, you must first enable it on the Security Management Server.

Enabling and Connecting to the ICA Management Tool

The ICA Management Tool is disabled by default.

To enable the ICA Management tool

Run this command on the Security Management Server:

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

The command options are:

Option	Description
on	Starts the ICA Management Tool (by opening port 18265)
off	Stops the ICA Management Tool (by closing port 18265)
-p	Changes the port used to connect to the CA (if the default port is not being used)
-a `"administrator DN" ...`	Sets the DNs of the administrators that will be allowed to use the ICA Management Tool
-u `"user DN" ...`	Sets the DNs of users allowed to use the ICA Management Tool. An option intended for administrators with limited privileges.

Note - If `cpca_client` is run without `-a` or `-u` parameters, the list of the allowed users and administrators remains unchanged.

To Connect to the ICA Management Tool

1. Add the administrator's certificate to the browser's certificate repository.
2. Open the ICA Management tool from the browser using this address:
   `https://<Management_Host_Name>:18265`
   Authenticate when requested.

The ICA Management Tool GUI

Item	Description
1	**Menu Pane** Shows a list of operations
2	**Operations Pane** **Manage certificates**. The window divides into **Search attributes configuration** and B**ulk operation configuration**. **Create Certificates**. **Configure the CA**. Contains configuration parameters You can also view the CA's time, name, and the version and build number of the Security Management Server. **Manage CRLs**. Download, publish, and recreate CRLs.
3	**Search Results Pane**. The results of the applied operation show in this pane. This window consists of a table with a list of certificates and certificate attributes.

Connect to the ICA Management tool using a browser and HTTPS connection.

Important: Before connecting, make sure to add an administrator certificate to the browser's store.

User Certificate Management

Internally managed User Certificates can be initialized, revoked or have their registrations removed using the ICA Management Tool. User Certificates of users managed on an LDAP server can only be managed using the ICA Management Tool.

This table shows User Certificate attributes that can be configured using the ICA Management Tool

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

Modifying the Key Size for User Certificates

If the user completes the registration from the Remote Access machine, the key size can be configured in the **Advanced Configuration** page in SmartConsole.

To configure the key size:

1. From the **Menu**, select **Global Properties**.
2. Go to Advanced, and in the **Advanced Configuration** section, click **configure**.
   The **Advanced Configuration** window opens.
3. Go to the **Certificates and PKI properties** page.
4. Set the new key size for this property: `user_certs_key_size`.
5. Click **OK**.

You can also change the key size using the GuiDBedit Tool (see sk13009 http://supportcontent.checkpoint.com/solutions?id=sk13009). Change the key size as it is listed in `users_certs_key_size Global Property`. The new value is downloaded when you update the site.

Performing Multiple Simultaneous Operations

The ICA Management Tool can do multiple operations at the same time. For example:

- Run an LDAP query for the details of all the organization's employees
- Create a file out of this data, and then use this file to:
  - Start (initialize) the creation of certificates for all employees
  - Send a notification about the new certificates to each of those employees

These operations can be done simultaneously:

- Start (initialize) user certificates
- Revoke user certificates
- Send mail to users
- Remove expired certificates
- Remove certificates for which the registration procedure was not completed

ICA Administrators with Reduced Privileges

The ICA Management Tool supports administrators with limited privileges. These administrators cannot execute multiple concurrent operations, and their privileges include only these:

- Basic searches
- Initialization of certificates for new users

Management of SIC Certificates

SIC certificates are managed using SmartConsole.

Management of Gateway VPN Certificates

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

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

Management of User Certificates in SmartConsole

The user certificates of users that are managed on the internal database are managed in SmartConsole.

For more information, see *User Certificates* in the *R80.10 Remote Access VPN Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=53105.

Notifying Users about Certificate Initialization

The ICA Management Tool can be configured to send a notification to users about certificate initialization. To send mail notifications

1. In the Menu pane, click **Configure the CA**.
2. In the **Management Tool Mail Attributes** area, configure:
   - The mail server
   - The mail "`From`" address
   - An optional '`To`' address, which can be used if the users' address is not known

     The administrator can use this address to get the certificates on the user's behalf and forward them later.
3. Click **Apply**.

Retrieving the ICA Certificate

For trust purposes, some gateways and remote clients, such as peer gateways that are not managed by the Security Management Server or clients using Clientless VPN, must retrieve the ICA certificate.

To retrieve the ICA Certificate:

1. Open a browser and enter the applicable URL.

   Use this format:

   `http://`*<Management Server IP address>*`:18264`

   The **Certificate Services** window opens.
2. Use the links to download the CA certificate to your computer or (in Windows) install the CA certification path.

Searching for a Certificate

There are two search options:

- A basic search that includes only the user name, type, status and the serial number
- An advanced search that includes all the search fields (can only be performed by administrators with unlimited privileges)

To do a certificate search:

In the **Manage Certificates** page, enter the search parameters, and click **Search**.

Basic Search Parameters

- **User Name** - Username string (by default, this field is empty)
- **Type** - a drop-down list with these options:
  - *Any* (default)
  - *SIC*
  - *Gateway*
  - *Internal User* or *LDAP user*
- **Status** - Drop-down list with these options:
  - *Any* (default)
  - *Pending*
  - *Valid*
  - *Revoked*
  - *Expired*
  - *Renewed (superseded)*
- **Serial Number** - Serial number of the requested certificate (by default, this field is empty)

Advanced Search Attributes

In addition to the parameters of the basic search, specify these parameters:

- **Sub DN** - DN substring (by default, this field is empty)
- **Valid From** - Date, from which the certificate is valid, in the format dd-mmm-yyyy [hh:mm:ss] (for example 15-Jan-2003) (by default, this field is empty)
- **Valid To** - Date until which the certificate is valid, in the format dd-mmm-yyyy [hh:mm:ss] (for example 14-Jan-2003 15:39:26) (by default, this field is empty)
- **CRL Distribution Point** - Drop-down list with these options:
  - *Any* (default)
  - *No CRL Distribution Point* (for certificates issued before the management upgrade - old CRL mode certificates)

  The list also shows all available CRL numbers.

The Search Results

The results of a search show in the **Search Results** pane. This pane consists of a table with a list of searched certificate attributes such as:

- **(SN) Serial Number** - The SN of the certificate
- **User Name (CN)** - The string between the first equals sign ("=") and the next comma (",")
- **DN**
- **Status** - One of these: *Pending, Valid, Revoked, Expired, Renewed (superseded)*
- The date from which certificates are valid until the date they expire

Note - The status bar shows search statistics after each search.

Viewing and Saving Certificate Details

You can view or save the certificate details that show in the search results.

To view and save certificate details:

Click on the **DN** link in the **Search Results** pane.

- If the status is *pending,* the certificate information together with the registration key shows, and a log entry is created and shows in SmartConsole > **Logs & Monitor** > **Logs**.
- If the certificate was already created, you can save it on a disk or open directly (if the operating system recognizes the file extension)

Removing and Revoking Certificates and Sending Email Notifications

1. In the Menu pane, click **Manage Certificates**.
2. Search for certificates ("Searching for a Certificate" on page 272) with set attributes.

   The results show in the **Search Results** pane.
3. Select the certificates, as needed, and click one of these options:
   - **Revoke Selected** - revokes the selected certificates and removes pending certificates from the CA's database
   - **Remove Selected** - removes the selected certificates from the CA's database and from the CRL

     Note - You can only remove expired or pending certificates.
   - **Mail to Selected -** sends mail for all selected *pending* certificates

     The mail includes the authorization codes. Messages to users that do not have an email defined are sent to a default address. For more, see Notifying Users about Certificate Initialization (on page 271).

Submitting a Certificate Request to the CA

There are three ways to submit certificate requests to the CA:

- **Initiate** - A registration key is created on the CA and used once by a user to create a certificate
- **Generate -** A certificate file is created and associated with a password which must be entered when the certificate is accessed
- **PKCS#10** - When the CA receives a PKCS#10 request, the certificate is created and delivered to the requester

To initiate a certificate:

1. In the Menu pane, select **Create Certificates > Initiate**.
2. Enter a **User Name** or **Full DN**, or click **Advanced** and fill in the form**:**
   - **Certificate Expiration Date** - Select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss] (the default value is two years from the date of creation)
   - **Registration Key Expiration Date** - Select a date or enter the date in the format dd-mmm-yyyy [hh:mm:ss] (the default value is two weeks from the date of creation)
3. Click **Go**.

   A registration key is created and show in the **Results** pane.

   If necessary, click **Send mail to user** to email the registration key. The number of characters in the email is limited to 1900.
4. The certificate becomes usable after entering the correct registration key.

To generate a certificate:

1. In the Menu pane, select **Create Certificates > Generate**.
2. Enter a **User Name** or **Full DN**, or click **Advanced** and fill in the form**:**
   - **Certificate Expiration Date** - Select a date or enter the date in the format dd-mm-yyyy [hh:mm:ss] (the default value is two years from the date of creation)
   - **Registration Key Expiration Date** - Select a date or enter the date in the format dd-mm-yyyy [hh:mm:ss] (the default value is two weeks from the date of creation)
3. Enter a password.
4. Click **Go**.
5. Save the P12 file, and supply it to the user.

To create a PKCS#10 certificate:

1. In the Menu pane, select **Create Certificates > PKCS#10**.
2. Paste into the space the encrypted base-64 buffer text provided.

   You can also click on **Browse for a file to insert (IE only)** to import the request file.
3. Click **Create** and save the created certificate.
4. Supply the certificate to the requester.

Initializing Multiple Certificates Simultaneously

You can initialize a batch of certificates at the same time.

To initialize several certificates simultaneously:

1. Create a file with the list of DNs to initialize.

   Note - There are two ways to create this file - through an LDAP query or a non-LDAP query.
2. In the Menu pain, go to **Create Certificates > Advanced**.
3. Browse to the file you created.
   - To send registration keys to the users, select **Send registration keys via email**
   - To receive a file that lists the initialized DNs with their registration keys, select **Save results to file**

     This file can later be used in a script.
4. Click **Initiate from file**.

Files created through LDAP Queries

The file initiated by the LDAP search has this format:

- Each line after a blank line or the first line in the file represents one DN to be initialized
- If the line starts with "`mail=`", the string continues with the mail of the user

  If no email is given, the email address will be taken from the ICA's "Management Tool Mail To Address" attribute.
- If there is a line with the `not_after` attribute, then the value at the next line is the Certificate Expiration Date

  The date is given in seconds from now.
- If there is a line with the is `otp_validity` attribute, then the value at the next line is the Registration Key Expiration Date.

  The date is given in seconds from now.

Here is an example of an LDAP Search output:

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

For more information, see User Directory ("LDAP and User Directory" on page 218).

Files created through a Simple Non-LDAP Query

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

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

CRL Management

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

- When approximately 60% of the CRL validity period has passed
- Immediately following the revocation of a certificate

It is possible to recreate a specified CRL using the ICA Management Tool. The utility acts as a recovery mechanism in the event that the CRL is deleted or corrupted. An administrator can download a DER encoded version of the CRL using the ICA Management Tool.

CRL Modes

The ICA can issue multiple CRLs. Multiple CRLs prevent one CRL from becoming larger than 10K. If the CRL exceeds 10K, IKE negotiations can fail when trying to open VPN tunnels.

Multiple CRLs are created by attributing each certificate issued to a specified CRL. If revoked, the serial number of the certificate shows in the specified CRL.

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

CRL Operations

You can download, update, or recreate CRLs through the ICA management tool.

To do operations with CRLs:

1. In the Menu pane, select **Manage CRLs**.
2. From the drop-down box, select one or more CRLs.
3. Select an action:
   - Click **Download** to download the CRL.
   - Click **Publish** to renew the CRL after changes have been made to the CRL database.

     This operation is done at an interval set by the **CRL Duration** attribute.
   - Click **Recreate** to recreate the CRL.

CA Cleanup

To clean up the CA, you must remove the expired certificates. Before you do that, make sure that the time set on the Security Management Server is correct.

To remove the expired certificates:

In the Menu pane, select **Manage CRLs > Clean the CA's Database and CRLs from expired certificates**.

Configuring the CA

To configure the CA:

1. In the Menu pane, select **Configure the CA**.
2. Edit the CA data values ("CA Data Types and Attributes" on page 277) as necessary.
3. In the **Operations** pane, select an operation:
   - **Apply** - Save and enter the CA configuration settings.

     If the values are valid, the configured settings become immediately effective. All non-valid strings are changed to the default values.
   - **Cancel** - Reset all values to the values in the last saved configuration.
   - **Restore Default** - Revert the CA to its default configuration settings.

     Entering the string `Default` in one of the attributes will also reset it to the default after you click **Configure**. Values that are valid will be changed as requested, and others will change to default values.

CA Data Types and Attributes

The CA data types are:

- **Time** - displayed in the format: `<number> days <number> seconds`, for example: `CRL Duration: 7 days 0 seconds`

  You can enter the values in the format in which they are displayed (`<number> days <number> seconds`) or as a number of seconds.
- **Integer** - a regular integer, for example: `SIC Key Size: 2048`
- **Boolean** - the values can be true or false (not case sensitive), for example: `Enable renewal: true`
- **String** - an alphanumeric string, for example: `Management Tool DN prefix: cn=tests`

These are the CA attributes, in alphabetical order:

Attribute	Comment	Values	Default
Authorization Code Length	The number of characters of the authorization codes.	min-6 max-12	6
CRL Duration	The period of time for which the CRL is valid.	min-5 minutes max-1 year	1 week
Enable Renewal	For User certificates. This is a Boolean value setting which stipulates whether to enable renewal or not.	true or false	true
Grace Period Before Revocation	The amount of time the old certificate will remain in Renewed (superseded) state.	*min-0* *max-5 years*	1 week

Attribute	Comment	Values	Default
Grace Period Check Period	The amount of time between sequential checks of the *Renewed (superseded)* list in order to revoke those whose duration has passed.	min-10 minutes max-1 week	1 day
IKE Certificate Validity Period	The amount of time an IKE certificate will be valid.	min-10 minutes max-20 years	5 years
IKE Certificate Extended Key Usage	Certificate purposes for describing the type of the extended key usage for IKE certificates. Refer to RFC 2459.		means no KeyUsage
IKE Certificate Key usage	Certificate purposes for describing the certificate operations. Refer to RFC 2459.		Digital signature and Key encipherment
Management Tool DN prefix	Determines the DN prefix of a DN that will be created when entering a user name.	possible values CN= UID=	CN=
Management Tool DN suffix	Determines the DN suffix of a DN that will be created when entering a user name.		ou=users
Management Tool Hide Mail Button	For security reasons the mail sending button after displaying a single certificate can be hidden.	true or false	false
Management Tool Mail Server	The SMTP server that will be used in order to send registration code mails. It has no default and must be configured in order for the mail sending option to work.		-
Management Tool Registration Key Validity Period	The amount of time a registration code is valid when initiated using the Management Tool.	min-10 minutes max-2 months	2 weeks

Attribute	Comment	Values	Default
Management Tool User Certificate Validity Period	The amount of time that a user certificate is valid when initiated using the Management Tool.	min-one week max-20 years	2 years
Management Tool Mail From Address	When sending mails this is the email address that will appear in the **from** field. A report of the mail delivery status will be sent to this address.		-
Management Tool Mail Subject	The email subject field.		-
Management Tool Mail Text Format	The text that appears in the body of the message. 3 variables can be used in addition to the text: `$REG_KEY` (user's registration key); `$EXPIRE` (expiration time); `$USER` (user's DN).		Registration Key: `$REG_KEY` `Expiration: $EXPIRE`
Management Tool Mail To address	When the **send** mail option is used, the emails to users that have no email address defined will be sent to this address.		-
Max Certificates Per Distribution Point	The maximum capacity of a CRL in the new CRL mode.	min-3 max-400	400
New CRL Mode	A Boolean value describing the CRL mode.	0 for old CRL mode 1 for new mode	true
Number of certificates per search page	The number of certificates that will be displayed in each page of the search window.	min-1 max-approx 700	approx 700
Number of Digits for Serial Number	The number of digits of certificate serial numbers.	min-5 max-10	5

Attribute	Comment	Values	Default
Revoke renewed certificates	This flag determines whether to revoke an old certificate after it has been renewed. The reason for not revoking this is to prevent the CRL from growing each time a certificate is renewed. If the certificate is not revoked the user may have two valid certificates.	true or false	true
SIC Key Size	The key size in bits of keys used in SIC.	possible values: 1024 2048 4096	2048
SIC Certificate Key usage	Certificate purposes for describing the certificate operations. Refer to RFC 2459.		Digital signature and Key encipherment
SIC Certificate Validity Period	The amount of time a SIC certificate will be valid.	min-10 minutes max-20 years	5 years
User Certificate Extended Key Usage	Certificate purposes for describing the type of the extended key usage for User certificates. Refer to RFC 2459.		means no KeyUsage
User Certificate Key Size	The key size in bits of the user's certificates.	Possible values: 1024 2048 4096	2048
User Certificate Key usage	Certificate purposes for describing the certificate operations. Refer to RFC 2459		Digital signature and Key encipherment

Certificate Longevity and Statuses

Certificates issued by the ICA have a defined validity period. When period ends, the certificate *expires*.

SIC certificates, VPN certificates for Security Gateways and User certificates can be created in one step in SmartConsole. User certificates can also be created in two steps using SmartConsole or the ICA Management Tool. The two steps are:

- Initialization – during this step a registration code is created for the user. When this is done, the certificate status is *pending*
- Registration – when the user completes the registration procedure in the remote client. After entering the registration code the certificate becomes *valid.*

The advantages are:

Enhanced security

- The private key is created and stored on the user's machine
- The certificate issued by the ICA is downloaded securely to the client.

Pre-issuance automatic and administrator-initiated certificate removal

If a user does not complete the registration procedure in a given period (two weeks by default), the registration code is automatically removed. An administrator can remove the registration key before the user completes the registration procedure. After that, the administrator can revoke the user certificate.

Explicit or Automatic Renewal of User certificates ensuring continuous User connectivity

A user certificate of type PKCS12 can be renewed explicitly by the user. A PKCS12 certificate can also be set to renew automatically when it is about to expire. This renewal operation ensures that the user can continuously connect to the organization's network. The administrator can choose when to set the automatic revoke old user certificates.

One more advantage is:

Automatic renewal of SIC certificates ensuring continuous SIC connectivity

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

Command Line Interface

See the *R80.20.M1 Command Line Interface Reference Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_CLI_ReferenceGuide/html_frameset.htm.