



Check Point
SOFTWARE TECHNOLOGIES LTD.

16 May 2017

NEXT GENERATION SECURITY GATEWAY R80.10

Guide

Classification: [Protected]



Check Point
SOFTWARE TECHNOLOGIES LTD.

INFINITY

© 2017 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page <http://www.checkpoint.com/copyright.html> for a list of our trademarks.

Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.

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.



Check Point R80.10

For more about this release, see the R80.10 home page
<http://supportcontent.checkpoint.com/solutions?id=sk111841>.



Latest Version of this Document

Download the latest version of this document
http://supportcontent.checkpoint.com/documentation_download?ID=54806.

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 Next Generation Security Gateway R80.10 Guide.



Searching in Multiple PDFs

To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package

<http://downloads.checkpoint.com/dc/download.htm?ID=54846>.

Use **Shift-Control-F** in Adobe Reader or Foxit reader.

Revision History

Date	Description
16 May 2017	First release of this document

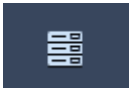
SmartConsole Toolbars

For a guided tour of SmartConsole, click **What's New** in the left bottom corner of SmartConsole.

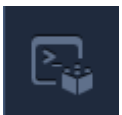
Global Toolbar (top left of SmartConsole)

	Description and Keyboard Shortcut
	The main SmartConsole Menu
	The Objects menu. Also leads to the Object Explorer Ctrl+E
	Install policy on managed gateways Ctrl+Shift+Enter

Navigation Toolbar (left side of SmartConsole)

	Description and Keyboard Shortcut
	Gateways & Servers configuration view Ctrl+1
	Security Policies Access Control view Security Policies Threat Prevention view Ctrl+2
	Logs & Monitor view Ctrl+3
	Manage & Settings view - review and configure the Security Management Server settings Ctrl+4

Command Line Interface Button (left bottom corner of SmartConsole)

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

What's New Button (left bottom corner of SmartConsole)

	Description and Keyboard Shortcut
	Open a tour of the SmartConsole

Objects and Validations Tabs (right side of SmartConsole)

	Description
Objects	Manage security and network objects
Validations	Validation warnings and errors

System Information Area (bottom of SmartConsole)

	Description
Task List	Management activities, such as policy installation tasks
Server Details	The IP address of the Security Management Server
Connected Users	The administrators that are connected to the Security Management Server

Contents

Important Information.....	3
SmartConsole Toolbars	4
Terms.....	11
Check Point Next Generation Security Gateway Solution.....	13
Overview of Firewall Features	13
How to Use this Guide	14
Components of the Check Point Firewall Solution	16
Creating an Access Control Policy	17
Introducing the Unified Access Control Policy	17
Creating a Basic Access Control Policy.....	18
Basic Rules.....	18
Use Case - Basic Access Control	19
Use Case - Inline Layer for Each Department.....	20
Creating Application Control and URL Filtering Rules.....	22
Monitoring Applications.....	22
Blocking Applications and Informing Users.....	23
Limiting Application Traffic	23
Using Identity Awareness Features in Rules	24
Blocking Sites.....	25
Blocking URL Categories.....	26
Ordered Layers and Inline Layers.....	27
The Need for Ordered Layers and Inline Layers	27
Order of Rule Enforcement in Inline Layers	28
Order of Rule Enforcement in Ordered Layers	29
Creating an Inline Layer	29
Creating a Ordered Layer	30
Enabling Access Control Features.....	31
Types of Rules in the Rule Base.....	32
Administrators for Access Control Layers.....	34
Sharing Layers	35
Visual Division of the Rule Base with Sections.....	35
Exporting Layer Rules to a .CSV File.....	35
Managing Policies and Layers	35
The Columns of the Access Control Rule Base	37
Source and Destination Column	37
VPN Column	38
Services & Applications Column.....	39
Content Column.....	42
Actions Column	43
Tracking Column	45
Unified Rule Base Use Cases	45
Use Case - Application Control and Content Awareness Ordered Layer	46
Use Case - Inline Layer for Web Traffic	47
Use Case - Content Awareness Ordered Layer.....	49
Use Case - Application Control and URL Filtering Ordered Layer.....	51
Rule Matching in the Access Control Policy	52
Examples of Rule Matching	52

Best Practices for Access Control Rules.....	55
Installing the Access Control Policy.....	56
Analyzing the Rule Base Hit Count.....	57
Enabling or Disabling Hit Count.....	57
Configuring the Hit Count Display.....	58
Preventing IP Spoofing.....	59
Configuring Anti-Spoofing	59
Anti-Spoofing Options.....	61
Translating IP Addresses (NAT).....	61
To Learn More About NAT	62
UserCheck Interactions in the Access Control Policy	62
Configuring the Security Gateway for UserCheck.....	62
Blocking Applications and Informing Users.....	64
UserCheck for Access Control Default Messages.....	65
Creating a UserCheck Interaction Object.....	65
Example UserCheck Message Using Field Variables	66
Localizing and Customizing the UserCheck Portal	66
UserCheck Frequency and Scope	67
UserCheck Settings	67
UserCheck CLI.....	69
Revoking Incidents	70
UserCheck Client.....	71
Blade Settings	79
Inspection Settings	79
Configuring Inspection Settings.....	79
Creating a Threat Prevention Policy	82
Threat Prevention Components	82
IPS.....	83
Anti-Bot	84
Anti-Virus	86
SandBlast	86
Assigning Administrators for Threat Prevention	88
Analyzing Threats	88
Out-of-the-Box Protection from Threats	89
Getting Quickly Up and Running with the Threat Prevention Policy.....	89
Enabling the Threat Prevention Software Blades	89
Installing the Threat Prevention Policy.....	92
Introducing Profiles.....	92
Optimized Protection Profile Settings.....	94
Predefined Rule.....	94
The Threat Prevention Policy	95
Workflow for Creating a Threat Prevention Policy.....	95
Threat Prevention Policy Layers.....	95
Threat Prevention Rule Base.....	97
Creating Threat Prevention Rules.....	98
Configuring IPS Profile Settings	98
Blocking Viruses.....	99
Configuring Anti-Bot Settings.....	100
Configuring Threat Emulation Settings	102
Configuring Threat Extraction Settings	106
Configuring a Malware DNS Trap	109
Exception Rules.....	109

The Check Point ThreatCloud.....	111
Updating IPS Protections.....	112
Scheduling Updates.....	112
Updating Threat Emulation.....	113
To Learn More About Threat Prevention.....	114
Creating Shared Policies.....	115
Shared Policies	115
Configuring HTTPS Inspection	116
Inspecting HTTPS Packets.....	117
Configuring Gateways to inspect outbound and inbound HTTPS.....	118
Configuring the Geo Policy.....	126
Adding Users to the Policy	129
Using Identity Awareness.....	129
Identity Sources.....	129
Enabling Identity Awareness	130
Working with Access Roles.....	132
Using Identity Awareness in the Access Control Policy	133
Redirecting to a Captive Portal	133
Sample Identity Awareness Rules	134
Using User Directory.....	134
User Directory Features	135
Deploying User Directory.....	135
Account Units	135
Working with LDAP Account Units	136
Enabling User Directory	139
Managing LDAP Information.....	139
To Learn More About Adding Users to the Policy.....	140
Logging and Monitoring	141
Log Analysis	141
Configuring Logging	141
Enabling Log Indexing	142
Sample Log Analysis	142
Tracking Options	143
Log Sessions	144
Views and Reports.....	145
Catalog of Views and Reports	146
Views.....	148
Reports.....	151
To Learn More About Logging and Monitoring.....	153
Maximizing Network Performance and Redundancy	154
Solutions for Enhancing Network Performance and Redundancy	154
CoreXL	155
Configuring CoreXL	155
To Learn More About CoreXL.....	155
SecureXL.....	156
Configuring SecureXL.....	156
To Learn More About SecureXL	157
Multi-Queue	157
ClusterXL	158
The Need for Clusters	158
ClusterXL Solution.....	158
IPv6 Support for ClusterXL	158

How ClusterXL Works.....	159
Installation and Platform Support	159
High Availability and Load Sharing in ClusterXL.....	159
Configuring ClusterXL.....	164
VRRP Cluster.....	168
How VRRP Failover Works.....	168
Internal Network High Availability.....	169
Preparing a VRRP Cluster	169
Configuring Monitored Circuit/Simplified VRRP - WebUI.....	171
Configuring the VRRP Security Gateway Cluster in SmartDashboard.....	173
Configuring VRRP Rules for the Security Gateway.....	173
To Learn More About Maximizing Network Performance.....	174
Simplifying Security for Private Clouds	175
Introduction to Virtual Systems (VSX)	175
VSX Overview.....	175
How VSX Works	175
VSX Architecture and Concepts.....	178
Virtual Devices.....	178
Interfaces	179
VSX Clusters.....	181
Configuring a VSX Cluster	184
An Example VSX cluster	184
Step 1 - Creating a VSX Cluster	185
Step 2 - Creating a Virtual Switch.....	188
Step 3 - Creating Virtual System 1.....	188
Step 4 - Creating Virtual System 2.....	190
Step 5 - Define the Policy on the Virtual Systems	190
To Learn More About VSX.....	190
Securing Data.....	191
Overview.....	191
Data Loss Prevention Features	191
Using a Mail Relay and Mail Server.....	192
Enabling DLP.....	192
Adding Data Owners	193
Notifying Data Owners	193
Using DLP with Microsoft Exchange	194
DLP Rule Base	194
Managing the DLP Rule Base.....	194
DLP Rule Exceptions	195
DLP Rule Actions	196
Sample Rule Base	197
Analyzing and Tracking DLP	197
Analyzing DLP Incidents in the Logs.....	198
Event Analysis Views Available in SmartConsole.....	198
To Learn More About Data Loss Prevention.....	198

Terms

Anti-Bot

1. An application that prevents computers from being controlled by hackers. 2. Check Point Software Blade that inspects network traffic for malicious bot software.

Anti-Virus

A solution to protect a computer or network against self-propagating programs or processes that can cause damage.

Block

1. To stop traffic before it reaches its destination. 2. To stop a command from execution. 3. To deny access by rule (though allowed by permission).

Bot

Malicious software that neutralizes Anti-Virus defenses, connects to a Command and Control center for instructions from cyber criminals, and carries out the instructions.

CoreXL

A performance-enhancing technology for Security Gateways on multi-core processing platforms.

Data Type

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

DLP

Data Loss Prevention. Detects and prevents the unauthorized transmission of confidential information.

Drop

To not allow packets through the gateway, blocking the connection.

Event

1. A record of a security incident that is based on one or more logs, and on a customizable set of rules that are defined in the Event Policy. 2. In Media Encryption, a device connects to an endpoint computer. 3. In SmartLSM, an object with schedule settings for the Security Gateway to fetch its security policy. 4. In Endpoint Security, an object with schedule settings for Active and Standby server synchronization.

Firewall

The software and hardware that protects a computer network by analyzing the incoming and outgoing network traffic (packets).

IKE

Internet Key Exchange. An Encryption key management protocol for IPSec that creates a shared key to encrypt and decrypt IP packets and establishes a VPN tunnel and Security Association.

IPS

Intrusion Prevention System. Check Point Software Blade that inspects and analyzes packets and data for numerous types of risks.

Performance Pack

Check Point product that accelerates IPv6 and IPv4 traffic. Installed on Security Gateways for significant performance improvements.

Remote Access Community

A group of computers, appliances, and devices that access, with authentication and encryption, the internal protected network from physically remote sites.

Remote Access VPN

An encryption tunnel between a Security Gateway and remote access clients, such as Endpoint Security VPN, and communities.

Rule

A set of traffic parameters and other conditions that cause specified actions to be taken for a communication session.

Rule Base

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

Security Gateway

A computer or an appliance that inspects traffic and enforces Security Policies for connected network resources.

Security Management Server

The server that manages, creates, stores, and distributes the security policy to Security Gateways.

Security Policy

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

SmartEvent Server

Physical server that hosts the events database.

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.

ThreatCloud Repository

A cloud database with more than 250 million Command and Control (C&C) IP, URL, and DNS addresses and over 2,000 different botnet communication patterns, used by the ThreatSpect engine to classify bots and viruses.

ThreatSpect Engine

A unique multi-tiered engine that analyzes network traffic and correlates data across multiple layers (reputation, signatures, suspicious mail outbreaks, behavior patterns) to detect bots and viruses.

UserCheck

Gives users a warning when there is a potential risk of data loss or security

violation. This helps users to prevent security incidents and to learn about the organizational security policy.

Check Point Next Generation Security Gateway Solution

In This Section:

Overview of Firewall Features	13
How to Use this Guide	14
Components of the Check Point Firewall Solution	16

Overview of Firewall Features

The Check Point Next Generation Security Gateway includes:

- Access Control
 - Firewall (network-level filtering)
 - Application Control
 - Internet access and filtering
 - Content Awareness
 - Site to Site VPN
 - Mobile Access and VPN Remote Access
- Intrusion and Threat Prevention
- Identity Awareness (network, user, and machine awareness, for Access Control and Threat Prevention)
- Data Loss Prevention

How to Use this Guide

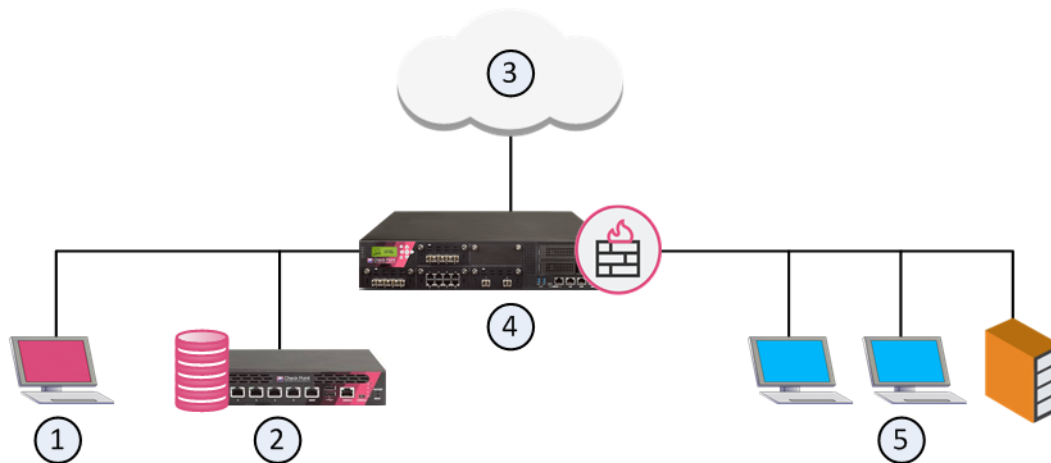
To configure an effective security solution, you must understand how to configure the Next Generation Security Gateway features, and how to add rules to your security policy. This guide helps you understand the general principles of the Check Point Next Generation Security Gateway, and how to configure it.

To learn more about each feature, look at the administration guide for the feature. There is a link to the appropriate administration guide at the end of each section of this guide. To find the link, search for "To Learn More".

Chapter		Feature	Section
Creating an Access Control Policy (on page 17)		Firewall	Basic Access Control ("Creating a Basic Access Control Policy" on page 18)
		Application Control	Creating a Unified Access Control Policy
		URL Filtering	
		Content Awareness	
		Mobile Access	
		IPsec VPN	
Creating a Threat Prevention Policy (on page 82)		IPS	
		Anti-Bot	
		Anti-Virus	
		Threat Emulation	
		Threat Extraction	
Creating Shared Policies (on page 115)		HTTPS Inspection	Configuring HTTPS Inspection (on page 116)
		Geo Control	Configuring the Geo Policy (on page 126)
Adding Users to the Policy (on page 129)		Identity Awareness	
Monitoring and Logging ("Logging and Monitoring" on page 141)		Logging & Status SmartEvent	

Chapter		Feature	Section
Maximizing Network Performance ("Maximizing Network Performance and Redundancy" on page 154)		Advanced Networking & Clustering	CoreXL (on page 155), SecureXL (on page 156) and Multi-Queue (on page 157) <i>Performance Tuning Administration Guide</i> http://downloads.checkpoint.com/dc/download.htm?ID=54765 ClusterXL (on page 158) and VRRP ("VRRP Cluster" on page 168)
Simplifying Security for Private Clouds (on page 175)		Virtual Systems	
Appendix: Securing Data ("Securing Data" on page 191)		Data Loss Prevention	

Components of the Check Point Firewall Solution



Item	Description
1	SmartConsole
2	Security Management Server
3	Internet and external networks
4	Security Gateway
5	Internal network

These are the primary components of a Check Point firewall solution:

- **Security Gateway** - The engine that enforces the organization's security policy, is an entry point to the LAN, and is managed by the Security Management Server.
- **Security Management Server** - The application that manages, stores, and distributes the security policy to Security Gateways.
- **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.

Creating an Access Control Policy

In This Section:

Introducing the Unified Access Control Policy.....	17
Creating a Basic Access Control Policy.....	18
Creating Application Control and URL Filtering Rules.....	22
Ordered Layers and Inline Layers	27
The Columns of the Access Control Rule Base	37
Unified Rule Base Use Cases.....	45
Rule Matching in the Access Control Policy	52
Best Practices for Access Control Rules	55
Installing the Access Control Policy	56
Analyzing the Rule Base Hit Count	57
Preventing IP Spoofing	59
Translating IP Addresses (NAT).....	61
UserCheck Interactions in the Access Control Policy	62
Blade Settings.....	79

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 Control and 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
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	General rules for the whole organization.
2	
3	An Inline Layer for the R&D department.
3.1	Rule 3 is the parent rules of the Inline Layer. The Action is the name of the Inline Layer.
3.2	
---	If a packet does not match on parent rule 3:
3.X	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	Another Inline Layer, for the QA department.
4.1	

4.Y	
5	More general rules for the whole organization.
--	One or more rules.
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 40) 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.

- Click one of the **Add Rule** toolbar buttons to add the rule in the position that you choose in the Rule Base.
- 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 39).

- 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 *access 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:

- 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.

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 *access 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 *access 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.....	27
Order of Rule Enforcement in Inline Layers	28
Order of Rule Enforcement in Ordered Layers	29
Creating an Inline Layer	29
Creating a Ordered Layer.....	30
Enabling Access Control Features	31
Types of Rules in the Rule Base	32
Administrators for Access Control Layers.....	34
Sharing Layers.....	35
Visual Division of the Rule Base with Sections	35
Exporting Layer Rules to a .CSV File	35
Managing Policies and Layers	35

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	https http	Allow
	2.2	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:

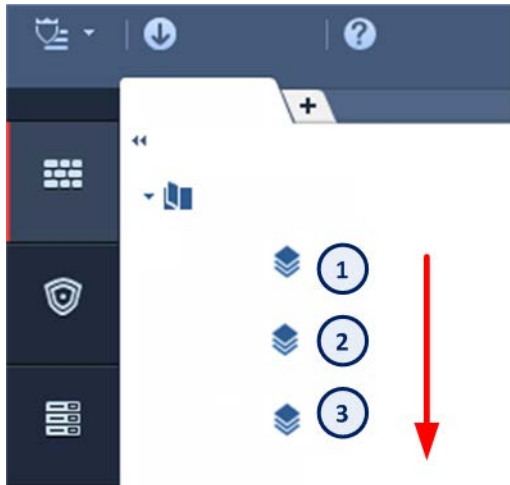
- If the packet matches a sub rule in the Inline Layer (Rule 2.1), no more rule matching is done.
- If none of the higher rules in the Ordered Layer match the packet, the explicit **Cleanup Rule** is applied (Rule 2.2). If this rule is missing, the **Implicit Cleanup Rule** ("Types of Rules in the Rule Base" on page 32) 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 32) 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 34).

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 Control and 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 32).
 - 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 32).

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 Control and 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 38).
 - Applications & URL Filtering ("**Services & Applications Column**" on page 39)
 - Content Awareness ("**Content Column**" on page 42)
 - Mobile Access ("**Mobile Access to the Network**" on page 38)

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 32).
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.

To learn how to configure administrator permissions for Layers, see the *R80.10 Security Management Administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54842>.

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 35).
- **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 57).
Name	Name that the system administrator gives this rule.
Source Destination	Network objects (" Source and Destination Column " on page 37) that define - Where the traffic starts - The destination of the traffic.
VPN	The VPN Community to which the rule applies (" VPN Column " on page 38).
Services & Applications	Services, Applications, Categories, and Sites (" Services & Applications Column " on page 39). If Application Control and 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 42). 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 43). 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 45).
Install On	Network objects that will get the rule(s) of the policy (" Installing the Access Control Policy " on page 56).
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
- Dynamic Objects
- Domain Objects
- Access Roles

To Learn More About Network Objects

To learn more about Network objects that you can add to the **Source** and **Destination** columns of the Access Control Policy, see the *R80.10 Security Management Administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54842>.

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 Mobile Access is enabled on a gateway, the gateway is automatically added to the **RemoteAccess** VPN Community. To make rules for the Mobile Access portal or client, include that Community, or a different one that includes the Mobile Access gateway, in the **VPN** column.

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 VPN and Remote Access, see these guides:

- *R80.10 VPN Site to Site Administration Guide*
http://supportcontent.checkpoint.com/documentation_download?ID=53104
- *R80.10 VPN Remote Access 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 31).

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 Control and 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	<i>Not relevant</i>	Customized
Any	<i>Not relevant</i>	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 Control and 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.
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.

Action	Meaning
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 ("UserCheck Interactions in the Access Control Policy" on page 62) 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 SmartDashboard). 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.

Tracking Column

These are some of the **Tracking** options (on page 143):

- **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.

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	46
Use Case - Inline Layer for Web Traffic	47
Use Case - Content Awareness Ordered Layer	49
Use Case - Application Control and URL Filtering Ordered Layer	51

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
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 <i>Cleanup Rule</i> is applied. The <i>Cleanup rule</i> 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 27). 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 Control and 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 <i>Potential_liability</i> group. The UserCheck <i>Blocked Message</i> is shown to users and explains why their traffic is blocked.						
2	High risk applications - Blocks traffic to sites and applications in the <i>High Risk</i> category and blocks the <i>iTunes</i> application. The UserCheck <i>Block Message</i> 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 <i>Radmin</i> application. Traffic that uses <i>Radmin</i> is allowed only during the <i>Work-Hours</i> (set to 8:00 through 18:30, for example).						
4	Allow Facebook for HR - Allows computers in the HR network to use <i>Facebook</i> . The total traffic downloaded from <i>Facebook</i> is limited to 1 Gbps, there is no upload limit.						
5	Block these categories - Blocks traffic to these categories: <i>Streaming Media</i> , <i>Social Networking</i> , <i>P2P File Sharing</i> , and <i>Remote Administration</i> . The UserCheck <i>Blocked Message</i> is shown to users and explains why their traffic is blocked. Note - The <i>Remote Administration</i> category blocks traffic that uses the <i>Radmin</i> application. If this rule is placed before rule 3, then this rule can also block <i>Radmin</i> for the IT department.						
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 55). 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
3	Any	Any	ftp	Any	Drop
4	Any	Any	Any	Any	Accept

This is the matching procedure when browsing an 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 *explicit 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 42): 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 45).

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**.

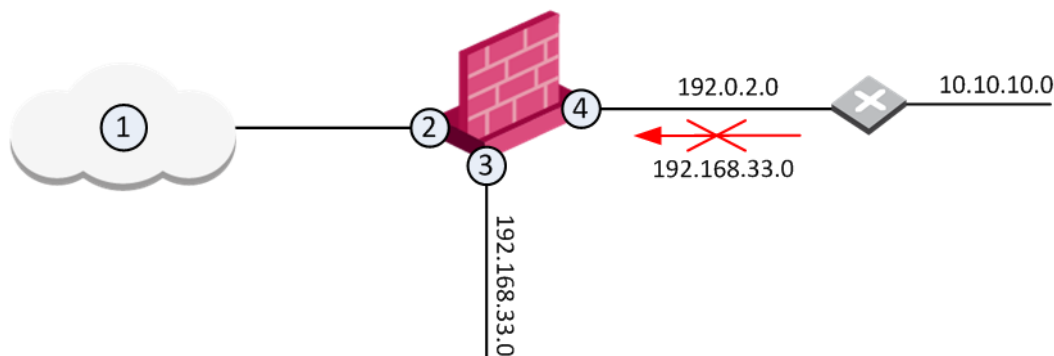
Preventing IP Spoofing

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 **General Properties** window of the Gateway 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, select **General**.

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

The **Topology Settings** window opens.

8. Select the type of network that the interface **Leads To**:

- **Internet (External)** or **This Network (Internal)** - This is the default setting. It is automatically calculated from the topology of the gateway. To update the topology of an internal network after changes to static routes, click **Network Management > Get Interfaces** in the **General Properties** window of the gateway.
- **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
 - **Specific** - A specific network 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, choose the zone of the interface.

10. Configure **Anti-Spoofing** options (on page 61). 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 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.

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.
- **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 to use Port Translation.

To Learn More About NAT

To learn more about NAT, see the *R80.10 Security Management Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54842>. Search for *Configuring the NAT Policy*.

UserCheck Interactions in the Access Control Policy

UserCheck objects lets the Security Gateway communicate with users. Use them in the Rule Base to:

- Help users with decisions that can be dangerous to the organization's security.
- Share the organization's changing internet policy for Web applications and sites with users, in real-time.

If a UserCheck object is set as the action on in a policy rule, the user's browser redirects to the UserCheck web portal on port 443 or 80. The portal shows the notifications to the user.

UserCheck client adds the option to send notifications for applications that are not in a web browser. The UserCheck client can also work together with the UserCheck portal to show notifications on the computer itself when the notification cannot be displayed in a browser.

Configuring the Security Gateway for UserCheck

Enable or disable UserCheck directly on the Security Gateway. Make sure that the UserCheck is enabled on each Security Gateway in the network.

The Security Gateway has an internal persistence mechanism that preserves UserCheck notification data if the Security Gateway or cluster reboots. Records of a user answering or receiving notifications are never lost.

To configure UserCheck on a Security Gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
The **Gateway Properties** window opens.

2. From the navigation tree, click **UserCheck**.
The **UserCheck** page opens.

3. Make sure **Enable UserCheck for active blades** is selected

4. In the **UserCheck Web Portal** section:

In the **Main URL** field, enter the primary URL for the web portal that shows the UserCheck notifications.

If users connect to the Security Gateway remotely, make sure that the Security Gateway internal interface (in the **Network Management** page) is the same as the Main URL.

Note - The **Main URL** field must be manually updated if:

- The Main URL field contains an IP address and not a DNS name.
- You change a gateway IPv4 address to IPv6 or vice versa.

5. **Optional:** Click **Aliases** to add URL aliases that redirect different hostnames to the **Main URL**.
The aliases must be resolved to the portal IP address on the corporate DNS server

6. In the **Certificate** section, click **Import** to import a certificate that the portal uses to authenticate to the Security Management Server.

By default, the portal uses a certificate from the Check Point Internal Certificate Authority (ICA). This might generate warnings if the user browser does not recognize Check Point as a trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority.

7. In the **Accessibility** section, click **Edit** to configure interfaces on the Security Gateway through which the portal can be accessed. These options are based on the topology configured for the Security Gateway. The topology must be configured.

Users are sent to the UserCheck portal if they connect:

- **Through all interfaces**
- **Through internal interfaces** (default)
 - **Including undefined internal interfaces**
 - **Including DMZ internal interfaces**
 - **Including VPN encrypted interfaces** (default)

Note: Make sure to add a rule to the Firewall Rule Base that allows the encrypted traffic.

- **According to the Firewall Policy.** Select this option if there is a rule that states who can access the portal.

If the **Main URL** is set to an external interface, you must set the **Accessibility** option to one of these:

- **Through all interfaces** - necessary in VSX environment
- **According to the Firewall Policy**

8. In the **Mail Server** section, configure a mail server for UserCheck. This server sends notifications to users that the Gateway cannot notify using other means, if the server knows the email address of the user. For example, if a user sends an email which matched on a rule, the Gateway cannot redirect the user to the UserCheck portal because the traffic is not http. If the user does not have a UserCheck client, UserCheck sends an email notification to the user.

- **Use the default settings** - Click the link to see which mail server is configured.
- **Use specific settings for this gateway** - Select this option to override the default mail server settings.
- **Send emails using this mail server** - Select a mail server from the list, or click **New** and define a new mail server.

9. Click **OK**.

10. If there is encrypted traffic through an internal interface, add a new rule to the Firewall Layer of the Access Control Policy. This is a sample rule:

Source	Destination	VPN	Services & Applications	Action
Any	Security Gateway on which UserCheck client is enabled	Any	UserCheck	Accept

11. Install the Access Control Policy.

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.

UserCheck for Access Control Default Messages

These are the default UserCheck messages in the **Access Tools > UserCheck** page of the Access Control Policy:

Name	Action Type	Description
Access Approval	Inform	
Access Notification	Inform	Shows when the action for the rule is inform. It informs users what the company policy is for that site.
Blocked Message - Access Control	Block	Shows when the action for the rule is Block, when a request is blocked.
Cancel Page - Access Control	Cancel	Shows after a user gets an Inform or Ask message and clicks Cancel.
Company Policy	Ask	Shows when the action for the rule is ask . It informs users what the company policy is for that site and they must click OK to continue to the site.

If the default UserCheck messages do not fit your needs, you can create a UserCheck Interaction object ("[Creating a UserCheck Interaction Object](#)" on page 65).

For example, you can create a message with Content Awareness fields (see "[Example UserCheck Message Using Field Variables](#)" on page 66).

You can show these UserCheck message previews:

- **Regular view** - Shows a preview of the UserCheck message on a computer.
- **Mobile** - Shows a preview of the UserCheck message on a mobile device.
- **Agent** - Shows a preview of the UserCheck message in the agent window.
- **Email** - Shows a preview of the UserCheck message in an email.

Creating a UserCheck Interaction Object

If the default UserCheck messages do not fit your needs, you can create a UserCheck Interaction object.

To create a UserCheck object that includes a message:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Click **Access Tools > UserCheck**.
3. Click **New**, and select one of these interaction modes:
 - **Ask UserCheck**- Show a message to users that asks them if they want to continue with the request or not.
 - **Block UserCheck**- Show a message to users and block the application request.
 - **Inform UserCheck** - Show an informative message to users. Users can continue to the application or cancel the request.

The **UserCheck Interaction** window opens on the **Message** page.

4. Enter a name for the UserCheck object and, optionally, a comment.

5. Select a language (English is the default) from the **Languages** tabs.
6. Enter the message content. You can:
 - Use the formatting toolbar to change text color, alignment, add or remove bullets.
 - Use the **Insert field** variables. These include fields for Content Awareness (see "[Example UserCheck Message Using Field Variables](#)" on page 66).
7. In the **Settings** tab, configure optional settings. For example:
 - **Fallback Action** - For a *Block* action type, when UserCheck notification cannot be displayed, this action is taken.
 - **External Portal** - When selected, redirects the user to the specified **External Portal** (enter the URL), and the UserCheck message is not shown to the end-user
Select **Add UserCheck Incident ID to the URL query**, to log the incident
8. Click **OK**.

This creates the UserCheck object and web page notification for the portal.

Example UserCheck Message Using Field Variables

If you define a custom UserCheck message ("[Creating a UserCheck Interaction Object](#)" on page 65), you can use predefined **Field** variables in the message.

Here is an example of a UserCheck message that you can define. This example uses some of the **Insert Field** variables for Application Control and Content Awareness rules:

According to the company policy, this action is intended for work-related use only.

Details:

- **File Name** is classified as **Data Types**
- Access to **Application name**
- Category **Category**

[] I will use this site/application and data in accordance with company policy.

Reference: **Incident ID**

Localizing and Customizing the UserCheck Portal

After you set the UserCheck interaction object language, you can translate the Portal **OK** and **Cancel** buttons to the applicable language. For more information, see sk83700 <http://supportcontent.checkpoint.com/solutions?id=sk83700>.

Some of the UserCheck predefined notifications are translated to more than one language. For example, **Access Notification** is translated to English, French, Spanish, and Japanese.

To support more languages:

1. In the Security Policies view of SmartConsole, go to the **Access Control** Policy.
2. Click **Access Tools > UserCheck**.
3. Double-click the UserCheck object to edit it.
4. In the **Message** page, click **Languages**.
5. Select the **Languages** from the list.

UserCheck Frequency and Scope

You can set the number of times that users get UserCheck messages for accessing applications that are not permitted by the policy. You can also set if the notifications are based on accessing the rule, application category, or application itself.

To set how often UserCheck notifications show:

1. Select the **Action** cell of a rule in the **Access Control Policy**, and click **More**.
2. In the **Action Settings** window, select the **UserCheck Frequency**.

The options are:

- **Once a day**
 - **Once a week**
 - **Once a month**
 - **Custom frequency**
3. Select **Confirm UserCheck**. This sets if the notifications are:
 - **Per rule**
 - **Per category**
 - **Per application**
 - **Per data type**

Example:

In a rule that contains:

Services & Applications	Action
Social Networking category	Inform

If you select a **UserCheck Frequency** of **Once a day**, and **Confirm UserCheck** of **Per rule**:

A user who accesses Facebook and then LinkedIn on the same day gets one Inform message.

If you select a **UserCheck Frequency** of **Once a day**, and **Confirm UserCheck** of **Per application**:

A user who accesses Facebook and then LinkedIn on the same day gets one Inform message for Facebook and one for LinkedIn.

In new installations, the **Confirm UserCheck Scope** default is **Per category**.

In upgrades from a version before R75.40, the **Confirm UserCheck** default is **Per Rule**.

UserCheck Settings

For each UserCheck interaction object you can configure these options from the **Settings** page UserCheck object:

- **Languages** - Set a language for the UserCheck message if the language setting in the user browser cannot be determined or is not implemented. For example:
 - If the browser native language is Spanish
 - The UserCheck message is in Japanese and French
 - You select Japanese as the default language

Then the notification displays in Japanese.

- **Fallback Action** (For Action Types **Ask** and **Inform**) - Select an alternative action (allow or block) for when the UserCheck notification cannot be shown in the browser or application that caused the notification. If UserCheck determines that the notification cannot be shown in the browser or application, the behavior is:
 - If the **Fallback Action** is **Allow** (the default for Inform messages), the user is allowed to access the website or application, and the UserCheck client (if installed) shows the notification.
 - If the **Fallback Action** is **Block**, the gateway tries to show the notification in the application that caused the notification. If it cannot and the UserCheck client is installed, it shows the notification through the client. The website or application is blocked, even if the user does not see the notification.
- **External Portal - Redirect the user to External Portal** - Select this to redirect users to an external portal, not on the gateway.
 - **URL** - Enter the URL for the external portal. The specified URL can be an external system that obtains authentication credentials from the user, such as a user name or password. It sends this information to the gateway.
 - **Add UserCheck Incident ID to the URL query** - An incident ID is added to the end of the URL query.
- **Conditions** (For the Action Type **Ask**) - Select actions that must occur before users can access the application. Select one or more of these options:
 - **User accepted and selected the confirm checkbox** - This applies if the UserCheck message contains a checkbox (**Insert User Input > Confirm Checkbox**). Users must accept the text shown and select the checkbox before they can access the application.
 - **User filled some textual input** - This applies if the UserCheck message contains a text field (**Insert User Input > Textual Input**). Users must enter text in the text field before they can access the application. For example, you might require that users enter an explanation for use of the application.

UserCheck CLI

You can use the `usrchk` command in the gateway command line to show or clear the history of UserCheck objects.

To use the `usrchk` commands, you must enable UserCheck on the gateway, and create a rule with a UserCheck interaction object.

Description `usrchk`
Syntax `usrchk [debug] [hits]`

Parameters

Parameter	Description
<code>debug</code>	Controls debug messages
<code>hits</code>	Shows user incident options: list - Options to list user incidents <code>all</code> - List all existing incidents. <code>user <username></code> - List incidents of a specified user. <code>uci <name of interaction object></code> - List incidents of a specified UserCheck interaction object clear - Options to clear user incidents <code>all</code> - Clear all existing incidents <code>user <username></code> - Clear incidents for a specified user <code>uci <name of interaction object></code> - Clear incidents of a specified UserCheck interaction object db - user hits database options

Examples:

- To show all UserCheck interaction objects, run: `usrchk hits list all`
- To clear the incidents for a specified user, run: `usrchk hits clear user <username>`

Notes:

- You can only run a command that contains `user <username>` if:
 - Identity Awareness is enabled on the gateway.
 - Identity Awareness is used in the same policy rules as UserCheck objects.
- To run a command that contains a specified UserCheck interaction object, first run `usrchk hits list all` to see the names of the interaction objects. Use the name of the interaction object as it is shown in the list.

Revoking Incidents

The Revoke Incidents URL can revoke a user's responses to UserCheck notifications. The URL is:

://<IP of gateway>/UserCheck/RevokePage

If users regret their responses to a notification and contact their administrator, the administrator can send users the URL.

After a user goes to the URL, all of the user's responses to notifications are revoked. The logs in the SmartConsole **Logs & Monitor** view **Logs** tab will show the user's activity, and that the actions were revoked afterwards.

Administrators can use the `usrchk` command of the CLI to revoke incidents for one user, all users, or a specified interaction object ("**UserCheck CLI**" on page 69).

UserCheck Client

The UserCheck client is installed on endpoint computers to communicate with the gateway and show UserCheck interaction notifications to users.

It works with these Software Blades:

DLP - Notifications of DLP incidents can be sent by email (for SMTP traffic) or shown in a popup from the UserCheck client in the system tray (for SMTP, HTTP and FTP).

- UserCheck client adds the option to send notifications for applications that are not in a web browser, such as Skype, iTunes, or browser add-ons (such as radio toolbars). The UserCheck client can also work together with the UserCheck portal to show notifications on the computer itself when:
- The notification cannot be displayed in a browser, or
- The UserCheck engine determines that the notification will not be shown correctly in the browser.

Users select an option in the notification message to respond in real-time.

For DLP, administrators with full permissions or the View/Release/Discard DLP messages permission can also send or discard incidents from the SmartConsole **Logs & Monitor Logs** view.

Workflow for installing and configuring UserCheck clients:

1. Configure how the clients communicate with the gateway and create trust with it.
2. Enable UserCheck and the UserCheck client on the gateway.
3. Download the UserCheck client MSI file.
4. Install the UserCheck client on the endpoint computers.
5. Make sure that the UserCheck clients can connect to the gateway and receive notifications.

UserCheck Requirements

See *UserCheck Client Requirements* in the *R80.10 Release Notes*
<http://downloads.checkpoint.com/dc/download.htm?ID=54802>.

Enabling UserCheck Client

Enable UserCheck and the UserCheck client on the gateway in the Properties window of the gateway object in SmartConsole. This is necessary to let clients communicate with the gateway.

To enable UserCheck and the UserCheck client on the 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, click **UserCheck**.
3. Select **Enable UserCheck for active blades**.
This enables UserCheck notifications from the gateway.
4. In the UserCheck Client section, select **Activate UserCheck Client support**.
This enables UserCheck notifications from the client.
5. Click **OK** and **Install Policy**.

Client and Gateway Communication

In an environment with UserCheck clients, the gateway acts as a server for the clients. Each client must be able to *discover* the server and create *trust* with it.

To create trust, the client makes sure that the server is the correct one. It compares the server fingerprint calculated during the SSL handshake with the expected fingerprint. If the server does not have the expected fingerprint, the client asks the user to manually confirm that the server is correct.

Here is a summary of the methods that you can use for clients to discover and trust the server. More details are described later in this section.

- **File name based server configuration** – If no other method is configured (default, out-of-the-box situation), all UserCheck clients downloaded from the portal are renamed to have the portal machine IP address in the filename. During installation, the client uses this IP address to connect to the gateway. Note that the user has to click **Trust** to manually trust the server.
- **AD based configuration** – If client computers are members of an Active Directory domain, you can deploy the server addresses and trust data using a dedicated tool.
- **DNS SRV record based server discovery** – Configure the server addresses in the DNS server. Note that the user has to click **Trust** to manually trust the server.
- **Remote registry** – All of the client configuration, including the server addresses and trust data reside in the registry. You can deploy the values before installing the client (by GPO, or any other system that lets you control the registry remotely). This lets you use the configuration when the client is first installed.

Option Comparison

	Requires AD	Manual User Trust (one time) Required?	Multi-Site	Client Remains Signed?	Still works after Gateway Changes	Level	Recommended for...
File name based	No	Yes	No	Yes	No	Very Simple	Single Security Gateway deployments
AD based	Yes	No	Yes	Yes	Yes	Simple	Deployments with AD that you can modify
DNS based	No	Yes	Partially (per DNS server)	Yes	Yes	Simple	Deployments without AD With an AD you cannot change, and a DNS that you can change
Remote registry	No	No	Yes	Yes	Yes	Moderate	Where remote registry is used for other purposes

File Name Based Server Discovery

This option is the easiest to deploy, and works out-of-the-box. It requires that users manually click **Trust** to trust the server the first time they connect. You can use this option if your deployment has only one Security Gateway with the relevant Software Blades.

How does it work?

When a user downloads the UserCheck client, the address of the Security Gateway is inserted in the filename. During installation, the client finds if there is a different discovery method configured (AD based, DNS based, or local registry). If no method is configured, and the gateway can be reached, it is used as the server. In the UserCheck Settings window, you can see that the server you connect to is the same as the Security Gateway in the UserCheck client filename.

Users must manually make sure that the trust data is valid, because the filename can be easily changed.

Renaming the MSI

You can manually change the name of the MSI file before it is installed on a computer. This connects the UserCheck client to a different gateway.

To rename the MSI file:

1. Make sure the gateway has a DNS name.
2. Rename the MSI using this syntax: **UserCheck_~GWname.msi**

Where *GWname* - is the DNS name of the gateway.

Optional: Use **UserCheck_~GWname-port.msi**

Where *port* is the port number of notifications. For example, **UserCheck_~mygw-18300.msi**.



Notes - The prefix does not have to be "UserCheck". The important part of the syntax is underscore tilde (_~), which indicates that the next string is the DNS of the gateway.

If you want to add the port number for the notifications to the client from the gateway, the hyphen (-) indicates that the next string is the port number.

Active Directory Based Configuration

If your client computers are members of an Active Directory domain and you have administrative access to this domain, you can use the Distributed Configuration tool to configure connectivity and trust rules.

The Distributed Configuration tool has three windows:

- **Welcome** - Describes the tool and lets you enter different credentials that are used to access the AD.
- **Server configuration** - Configure which Security Gateway the client connects to, based on its location.
- **Trusted gateways** - View and change the list of fingerprints that the Security Gateways consider secure.

To enable Active Directory based configuration for clients:

1. Download and install the UserCheck client MSI on a computer.

From the command line on that computer, run the client configuration tool with the AD utility.

For example, on a Windows 7 computer:

```
"C:\Users\<user name>\Local Settings\Application
Data\Checkpoint\UserCheck\UserCheck.exe" -adtool
```

The Check Point UserCheck - Distributed Configuration tool opens.

2. In the **Welcome** page, enter the credentials of an AD administrator.

By default, your AD username is shown. If you do not have administrator permissions, click **Change user** and enter administrator credentials.

3. In the **Server Configuration** page, click **Add**.

The **Identity Server Configuration** window opens.

4. Select **Default** and then click **Add**.

5. Enter the IP address or Fully Qualified Domain Name (FQDN) and the port of the Security Gateway.

6. Click **OK**.

The identity of the AD Server for the UserCheck client is written in the Active Directory and given to all clients.

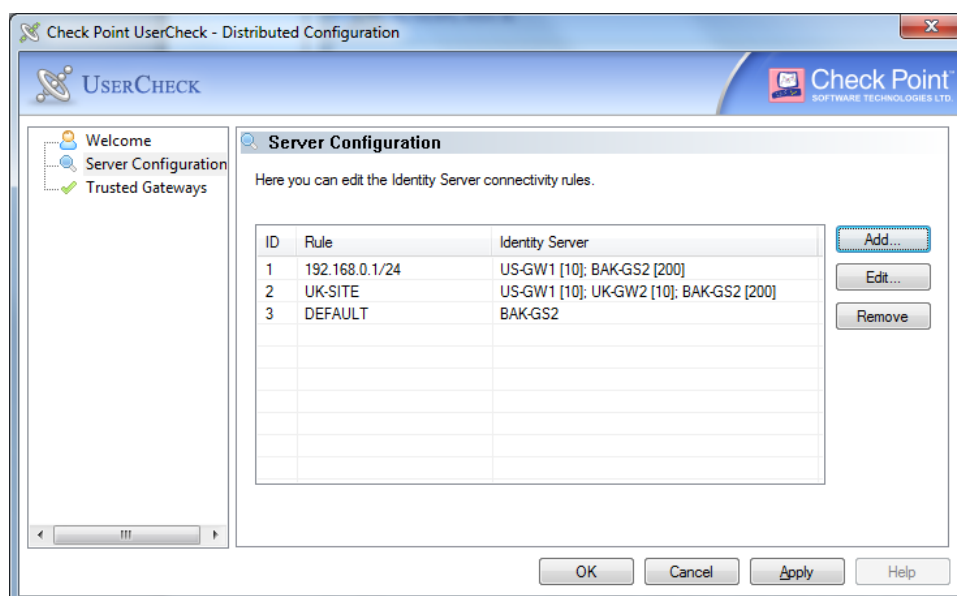


Note - The entire configuration is written under a hive named **Check Point** under the **Program Data** branch in the AD database that is added in the first run of the tool. Adding this hive does not affect other AD based applications or features.

Server Configuration Rules

If you use the Distributed Configuration tool and you configure the client to **Automatically discover** the server, the client fetches the rule lists. Each time it must connect to a server, it tries to match itself against a rule, from top to bottom.

When the tool matches a rule, it uses the servers shown in the rule, according to the priority specified.



The configuration in this example means:

1. If the user is coming from '192.168.0.1 - 192.168.0.255', then try to connect to US-GW1. If it is not available, try BAK-GS2 (it is only used if US-GW1 is not available, as its priority is higher).

2. If the user is connected from the Active Directory site 'UK-SITE', connect either to UK-GW1 or UK-GW2 (choose between them randomly, as they both have the same priority). If both of them are not available, connect to BAK-GS2.
3. If rules 1 and 2 do not apply, connect to BAK-GS2 (the default rule is always matched when it is encountered).

Use the **Add**, **Edit** and **Remove** buttons to change the server connectivity rules.

Trusted Gateways

The **Trusted Gateways** window shows the list of servers that are trusted - no messages open when users connect to them.

You can add, edit or delete a server. If you have connectivity to the server, you can get the name and fingerprint. Enter its IP address and click **Fetch Fingerprint** in the **Server Trust Configuration** window. If you do not have connectivity to the server, enter the same name and fingerprint that is shown when you connect to that server.

DNS Based Configuration

If you configure the client to **Automatic Discovery** (the default), it looks for a server by issuing a DNS SRV query for the address of the gateway (the DNS suffix is added automatically). You can configure the address in your DNS server.

To configure DNS based configuration on the DNS server:

1. Go to **Start > All Programs > Administrative Tools > DNS**.
2. Go to **Forward lookup zones** and select the applicable domain.
3. Go to the **_tcp** subdomain.
4. Right click and select **Other new record**.
5. Select **Service Location, Create Record**.
6. In the **Service** field, enter **CHECKPOINT_DLP**.
7. Set the **Port number** to 443.
8. In **Host offering this server**, enter the IP address of the Security Gateway.
9. Click **OK**.

To configure Load Sharing for the Security Gateway, create multiple SRV records with the same priority.

To configure High Availability, create multiple SRV records with different priorities.



Note - If you configure AD based and DNS based configuration, the results are combined according to the specified priority (from the lowest to highest).

Troubleshooting DNS Based Configuration

To troubleshoot issues in DNS based configuration, you can see the SRV records that are stored on the DNS server.

To see SRV records on the DNS server:

Run:

```
C:\> nslookup
> set type=srv
> checkpoint_dlp._tcp
```

The result is:

```
C:\> nslookup
> set type=srv
> checkpoint_dlp._tcp
Server:  dns.company.com
Address: 192.168.0.17
checkpoint_dlp._tcp.ad.company.com    SRV service location:
      priority      = 0
      weight        = 0
      port          = 443
      svr hostname  = dlpserver.company.com
dlpserver.company.com internet address = 192.168.1.212
>
```

Remote Registry

If you have a way to deploy registry entries to your client computers, for example, Active Directory or GPO updates, you can deploy the Security Gateway addresses and trust parameters before you install the clients. Clients can then use the deployed settings immediately after installation.

To configure the remote registry option:

1. Install the client on one of your computers. The agent installs itself in the user directory, and saves its configuration to HKEY_CURRENT_USER.
2. Connect manually to all of the servers that are configured, verify their fingerprints, and click **Trust** on the fingerprint verification dialog box.
3. Configure the client to manually connect to the requested servers (use the **Settings** window).
4. Export these registry keys (from HKEY_CURRENT_USER):
 - a) SOFTWARE\CheckPoint\UserCheck\TrustedGateways (the entire tree)
 - b) SOFTWARE\CheckPoint\UserCheck\
 - (i) DefaultGateway
 - (ii) DefaultGatewayEnabled
5. Import the exported keys to the endpoint computers before you install the UserCheck client.

Getting the MSI File

To get the MSI file:

1. In SmartConsole, in the **Gateways & Servers** view, open the **General Properties** window of the gateway object.
2. From the navigation tree, select **UserCheck**.
3. In the **UserCheck Client** section, click **Download Client**.



Important - Before you can download the client msi file, the UserCheck portal must be up. The portal is up only after a Policy installation.

Distributing and Connecting Clients

After configuring the clients to connect to the gateway, install the clients on the user machines. You can use any method of MSI or EXE mass deployment and installation that you choose. For example, you can send users an email with a link to install the client. When a user clicks the link, the MSI file automatically installs the client on the computer.

Alternatively, users can download the installation package from the regular DLP UserCheck notifications.

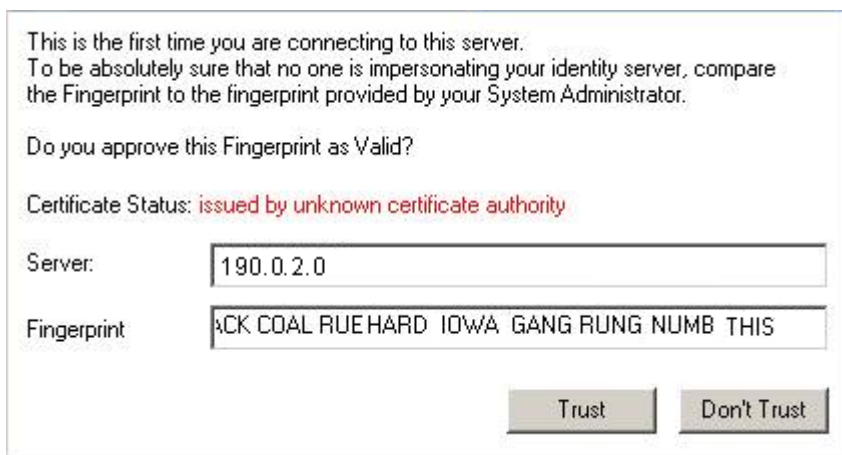
To install the client for all user accounts on a Windows computer, see sk96107

<http://supportcontent.checkpoint.com/solutions?id=sk96107>.

The installation is silent and generally, no reboot is required.

When the client is first installed, the tray icon indicates that it is not connected. When the client connects to the gateway, the tray icon shows that the client is active.

The first time that the client connects to the gateway, it asks for verification from the user and approval of the fingerprint.



Best Practices:

- Let the users know this will happen.
- Use a server certificate that is trusted by the certificate authority installed on users' computers. Then users do *not* see a message that says: **Issued by unknown certificate authority**.

If UserCheck for DLP is enabled on the gateway, users are required to enter their username and password after the client installs.

Example of message to users about the UserCheck client installation (for DLP):

Dear Users,

Our company has implemented a Data Loss Prevention automation to protect our confidential data from unintentional leakage. Soon you will be asked to verify the connection between a small client that we will install on your computer and the computer that will send you notifications.

This client will pop up notifications if you try to send a message that contains protected data. It might let you to send the data anyway, if you are sure that it does not violate our data-security guidelines.

When the client is installed, you will see a window that asks if you trust the DLP server. Check that the server is SERVER NAME and then click Trust.

In the next window, enter your username and password, and then click OK.



Note - If the UserCheck client is not connected to the gateway, the behavior is as if the client was never installed. Email notifications are sent for SMTP incidents and the Portal is used for HTTP incidents.

UserCheck and Check Point Password Authentication

You can see and edit Check Point users from **Users and Administrators** in the navigation tree.

To enable Check Point password authentication:

SmartConsole Configuration

1. Open SmartConsole and open the **Manage & Settings** view.
2. Click **Permissions & Administrators > Administrators**, and select an existing user or create a new user.
3. In the **General Properties** page of the user, make sure that an email address is defined.
4. In the **Authentication Properties** page of the user, set **Authentication Scheme** to **Check Point Password** and enter the password and password confirmation.
5. Click **OK**.

UserCheck Client Configuration

Ask your users to configure their UserCheck client:

1. On the UserCheck client computer, right click the UserCheck icon in the Notification Area (next to the system clock).
2. Select **Settings**.
3. Click **Advanced**.
4. Select **Authentication with Check Point user accounts defined internally in SmartDashboard**.

Helping Users

If users require assistance to troubleshoot issues with the UserCheck client, you can ask them to send you the logs.

To configure the client to generate logs:

1. Right-click the UserCheck tray icon and select **Settings**.
The **Settings** window opens.
2. Click **Log to** and browse to a pathname where the logs are saved.
3. Click **OK**.

To send UserCheck logs from the client:

1. Right-click the UserCheck tray icon and select **Status**.
The **Status** window opens.
2. Click **Advanced** and then click the **Collect information for technical support** link.
The default email client opens, with an archive of the collected logs attached.

Blade Settings

To configure **Global Properties**, **Inspection Settings** and **Advanced Settings** for **Blades**:

1. In SmartConsole, go to the **Manage & Settings** view.
2. Click **Blades**.

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 SmartDashboard, 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.

Creating a Threat Prevention Policy

In This Section:

Threat Prevention Components	82
Assigning Administrators for Threat Prevention	88
Analyzing Threats	88
Out-of-the-Box Protection from Threats	89
The Threat Prevention Policy	95
Creating Threat Prevention Rules	98
The Check Point ThreatCloud	111
To Learn More About Threat Prevention	114

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.
- Up to 15 Gbps throughput with optimized security, and up to 2.5 Gbps throughput with all IPS protections activated
- #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.

For more about how to configure administrator permissions, see the *R80.10 Security Management Administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54842>.

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, that 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.....	89
Enabling the Threat Prevention Software Blades	89
Installing the Threat Prevention Policy	92
Introducing Profiles	92
Optimized Protection Profile Settings	94
Predefined Rule	94

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 [94](#)) 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 [92](#)).

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 92).

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 92).

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 **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 92).

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 **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 <i>Medium or lower</i> effect on performance.
Protect against important threats	Severity	Protect against threats with a severity of <i>Medium or above</i> .
Reduce false-positives	Confidence	Set to <i>Prevent</i> the protections with an attack <i>confidence</i> of <i>Medium or High</i> . Set to <i>Detect</i> the protections with a confidence of <i>Low</i> .

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	95
Threat Prevention Policy Layers	95
Threat Prevention Rule Base	97

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 Threat Prevention Policy Layers.

Note - For each Policy Layers, configure a Threat Prevention Rule Base with the Threat Prevention profile as the *Action* of the rule.

4. Install the Threat Prevention policy.

Threat Prevention Policy Layers

With R80.10 Gateways, you can create a Threat Prevention Rule Base with multiple Ordered Layers. Each Ordered Layer calculates its action separately from the other Layers. When a connection matches rules in more than one Layer, the gateway enforces the strictest action and settings.

For your convenience, you can divide the Ordered Layers by Software Blades, services or networks.

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 how the Threat Prevention Software Blade resolves conflicting actions in different Layer.

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.

Threat Prevention Layers in Pre-R80 Gateways

When you upgrade to R80 or higher from earlier versions:

Gateways that have the IPS and Threat Prevention Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention. The IPS Layer includes the ThreatCloud IPS protections. Core IPS protections stay in the Access Control Policy.

Best Practice - For better performance, we recommend to use the Optimized profile when you upgrade to R80 or higher from earlier versions.

You can add more Layer to the two Layer created during upgrade ("[Managing Policies and Layers](#)" on page 35).

All layers are evaluated in parallel.

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 ("[Using Identity Awareness](#)" on page 129) 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:

Configuring IPS Profile Settings	98
Blocking Viruses	99
Configuring Anti-Bot Settings	100
Configuring Threat Emulation Settings	102
Configuring Threat Extraction Settings	106
Configuring a Malware DNS Trap	109
Exception Rules	109

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.
 8. If you are importing 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 are in staging mode until their configuration is changed. 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

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 92).

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 92).

Disabling a Protection on a Specified 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.
 - **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.

Note - The MIME Nesting settings are the same for Anti-Virus, Threat Emulation and Threat Extraction.

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:
7. Select the applicable **Protocols** to be emulated.
8. 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.
9. **Optional:** Configure how Threat Emulation does emulation for SMTP traffic.
 - a) Click **Configure**.
The **Threat Prevention Mail Configuration** window opens.
 - b) Configure the **MIME Nesting** settings.
 - **Maximum MIME nesting is X levels** - For emails that contain nested MIME content, Set the maximum number of levels that the ThreatSpect engine scans in the email.
 - **When nesting level is exceeded block/allow file** - If there are more nested levels of MIME content than the configured amount, select to **Block** or **Allow** the email file.
10. Select the **File Types** to be emulated.
11. Click **OK** and close the Threat Prevention profile window.
12. 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.

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



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 Threat Emulation:

1. From the Threat Prevention profile navigation tree, select **Threat Emulation > Excluded Mail Addresses**.
2. 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 are not sent for emulation.
3. 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 are not sent for emulation.

4. Click **OK** and close the Threat Prevention profile window.
5. 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.

Using Local or Remote Emulation

This section is for deployments that use an Emulation appliance and run emulation in the internal network.



Note - Prepare the network for the Emulation appliance before you run the First Time Configuration Wizard ("[Preparing for Local or Remote Emulation](#)" on page 105).

To enable an Emulation appliance for Local and Remote emulation:

1. In SmartConsole, go to **Gateways & Servers** and double-click the Emulation appliance.
The **Gateway Properties** window opens.
2. From the **Network Security** tab, select **Threat Emulation**.
The **Threat Emulation First Time Configuration Wizard** opens and shows the **Emulation Location** page.
3. Select **Locally on a Threat Prevention device**.
4. Click **Next**.
The **Summary** page opens.
5. Click **Finish** to enable Threat Emulation on the Emulation appliance and close the First Time Configuration Wizard.
6. Click **OK**.
The **Gateway Properties** window closes.
7. For Local emulation, install the Threat Prevention policy on the Emulation appliance.

To enable Threat Emulation on the Security Gateway for Remote emulation:

1. In SmartConsole, go to **Gateways & Servers** and double-click the Security Gateway.
The **Gateway Properties** window opens.
2. From the **Network Security** tab, select **Threat Emulation**.
The **Threat Emulation First Time Configuration Wizard** opens and shows the **Emulation Location** page.

3. Configure the Security Gateway for Remote Emulation:
 - a) Select **Other Emulation appliance**.
 - b) From the drop-down menu, select the Emulation appliance.
4. Click **Next**.
The **Summary** page opens.
5. Click **Finish** to enable Threat Emulation on the Security Gateway close the First Time Configuration Wizard.
6. Click **OK**.
The **Gateway Properties** window closes.
7. Install the Threat Prevention policy on the Security Gateway and 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. On the **Threat Extraction > General** page, configure:

UserCheck Settings

- **Allow the user to access the original file**
- **Allow access to original files that are not malicious according to Threat Emulation**

Note - This option is only configurable when the Threat Emulation blade is activated in the **General Properties** pane of the profile.

- **UserCheck Message**

Select a message to show the user when the user receives the clean file. In this message, the user selects if they want to download the original file or not. To select the success or cancelation messages of the file download, go to Manage & Settings > **Blades > Threat Prevention > Advanced Settings > UserCheck**. You can create or edit UserCheck messages on the UserCheck page.

- Optional: To give the user access to the original email, click **Insert Field**, and select **Send Original Mail**.

Send Original Mail is added to the message body.

Protocols

- **Mail (SMTP)**

Click **Configure** to set the maximum MIME nesting level for emails that contained nested MIME content.

Extraction Method

- **Extract files from potential malicious parts** - Selected by default

Click **Configure** to select which malicious parts the blade extracts. For example, macros, JavaScript, images and so on.

- **Convert to PDF -**

Converts the file to PDF, and keeps text and formatting.

Best Practice - If you use PDFs in right-to-left languages or Asian fonts, preferably select **Extract files from potential malicious parts** to make sure that these files are processed correctly.

Extraction Settings

- **Process all files** - selected by default
- **Process malicious files when the confidence level is:**

Set a low, medium or high confidence level. This option is only configurable when the Threat Emulation blade is activated in the **General Properties** pane of the profile.

File Types

- **Process all supported file types** - selected by default
- **Process specific file type families -**

Click **Configure** to select if you want Threat Extraction support for only some file types from the list. This list includes only specified file types that the administrator selected. To change the selection, go to the **Manage & Settings** view > **Blades** > **Threat Prevention** > **Advanced Settings** > **Threat Extraction** > **Configure File Type Support**.

Notes:

- For jpg, bmp, png, gif, and tiff files - Threat Extraction supports only extraction of potentially malicious content.
- For hwp, jtd, eps, files - Threat Extraction supports only conversion to pdf.
- For Microsoft Office and PDF files and all other file types on the list - Threat Extraction supports both extraction of potentially malicious content and conversion to pdf.
- You can also configure supported file types in the configuration file. For explanation, see sk112240 <http://supportcontent.checkpoint.com/solutions?id=sk112240>.

5. On the **Exclude/Include Users** page, configure these settings:

- **Scan all emails** - selected by default

Click **Exceptions** to not include specified users, groups, recipients or senders.

- **Scan mail only for specific users or groups**

Click **Configure** to select specified User Groups, Recipients or Senders.

Note:

A *user* is an object that can contain an email address with other details.

A *group* is an AD group or LDAP group of users

A *recipient* is an email address only.

Important: In the **Application menu** > **Global Properties** > **User Directory**, make sure that you have selected the **Use User Directory for Security Gateways** option.

6. In **Threat Tools** > **Profiles** > **Threat Extraction** > **Advanced**, configure these settings:

Logging

- **Log only those files from which threats were extracted** - selected by default
- **Log every file**

Threat Extraction Exceptions

- **Corrupted attachments**

Block or Allow corrupted files attached to the email. Corrupted files are files the blade fails to process, possibly because the format is incorrect. Despite the incorrect format, the related application (Word, Adobe Reader) can sometimes show the content.

Block removes the corrupt attachment and sends the recipient a text describing how the attachment contained potentially malicious content. You can block corrupt files if they are malicious according to Threat Emulation. If the action is block, you can deny access to the original corrupted file.

Allow lets the recipient receive the corrupt file attachment.

- **Encrypted attachments**

Block or Allow encrypted files attached to the email.

Block removes the encrypted attachment and sends the recipient a text file describing how the attachment contained potentially malicious content.

If the action is block, you can also deny access to the original encrypted file.

Allow lets the recipient receive the encrypted attachment.

- **Signed emails**

Allow or Clean signed emails.

Signed emails are not encrypted, but the mail contents are *signed* to authenticate the sender. If the received email differs from the email that was sent, the recipient gets a warning. The digital signature is no longer valid.

Clean replaces the original attachment with an attachment cleaned of threats, or converts the attachment to PDF form. Both actions invalidate the digital signature. If the attachment does not include active content, the mail remains unmodified and the digital signature valid.

Allow does not change the email. The digital signature remains valid. Select this option to prevent altering digital signatures.

7. 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:

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, choose one of the options:
 - **According to profile settings** - Use the Malware DNS Trap IP address configured for each profile.
 - **IPv4** - Enter the IP address for 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**.

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:

Updating IPS Protections	112
Scheduling Updates	112
Updating Threat Emulation	113

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 using SmartConsole (if your Security Management Server has no internet access), or
 - Download using Security Management Server.
4. **Install Policy**.

To manually 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**, click the drop-down menu.
4. Select **Offline Update**.
The file directory opens.
5. Select the required file for the update and click **Open**.
6. **Install Policy**.

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>.

Creating Shared Policies

In This Section:

Shared Policies	115
Configuring HTTPS Inspection	116
Configuring the Geo Policy	126

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.
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 <i>R80.10 Next Generation Security Gateway Guide</i> http://downloads.checkpoint.com/dc/download.htm?ID=54806.
Inspection Settings	You can configure Inspection Settings (on page 79) for the Firewall: • Deep packet inspection settings • Protocol parsing inspection settings • VoIP packet inspection settings

Configuring HTTPS Inspection

HTTPS Internet traffic uses the SSL (Secure Sockets Layer) protocol and is encrypted to give data privacy and integrity. However, HTTPS traffic has a possible security risk and can hide illegal user activity and malicious traffic. Security Gateways cannot inspect HTTPS traffic because it is encrypted. You can enable the HTTPS Inspection feature to let the Security Gateways create new SSL connections with the external site or server. The Security Gateways are then able to decrypt and inspect HTTPS traffic that uses the new SSL connections.

There are two types of HTTPS Inspection:

- **Outbound HTTPS Inspection** - To protect against malicious traffic that is sent from an internal client to an external site or server.
- **Inbound HTTPS Inspection** - To protect internal servers from malicious requests that arrive from the Internet or an external network.

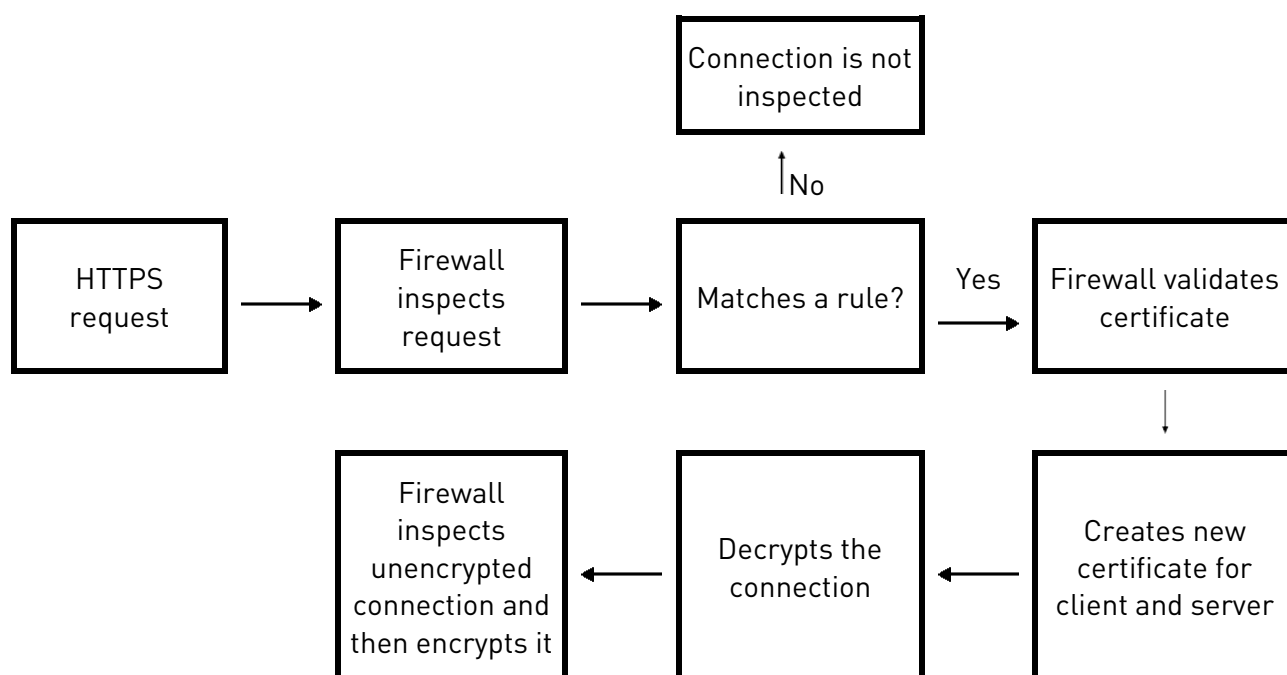
A Security Gateway uses certificates and becomes an intermediary between the client computer and the secure web site. All data is kept private in HTTPS Inspection logs. Only administrators with HTTPS Inspection permissions can see all the fields in such a log.

Inspecting HTTPS Packets

Outbound Connections

Outbound connections are HTTPS connections that arrive from an internal client and connect to the Internet. The Security Gateway compares the HTTPS request to the rules in the HTTPS Inspection Rule Base. If the request does not match any rule, the packet is not inspected and the connection is allowed.

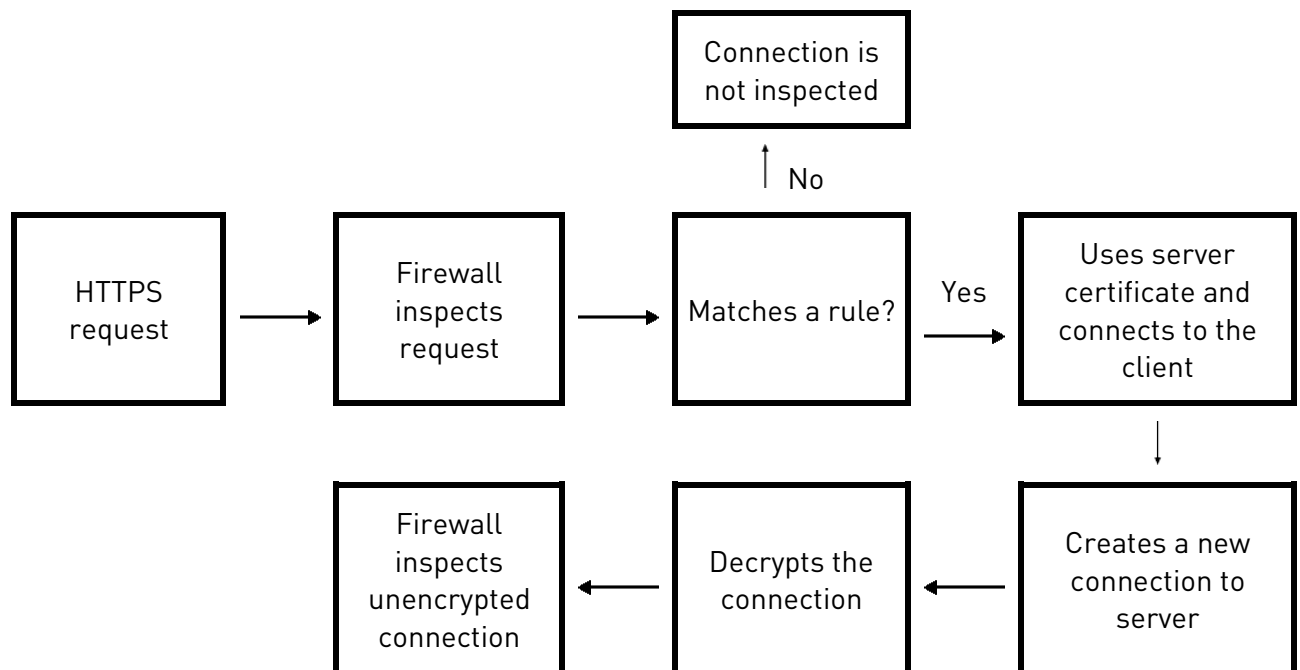
If the request matches an HTTPS Inspection rule, the Security Gateway validates the certificate from the server (on the Internet). The Security Gateway validates the certificate using the Online Certificate Status Protocol (OCSP) standard. OCSP is faster and uses much less memory than CRL Validation, which is used for certificate validation in releases lower than R80.10. For a new HTTPS connection to the server, the Security Gateway creates and uses a new certificate. There are two HTTPS connections, one to the internal client and one to the external server. It can then decrypt and inspect the packets according to the security policy. The packets are encrypted again and sent to the destination.



Inbound Connections

Inbound connections are HTTPS connections that arrive from an external client and connect to a server in the DMZ or the internal network. The Security Gateway compares the HTTPS request to the rules in the HTTPS Inspection Rule Base. If the request does not match any rule, the packet is not inspected and the connection is allowed.

If the request matches an HTTPS Inspection rule, the Security Gateway uses the certificate for the internal server to create an HTTPS connection with the external client. The Security Gateway creates a new HTTPS connection with the internal server. Since the Security Gateway has a secure connection with the external client, it can decrypt the HTTPS traffic. The decrypted traffic is inspected according to the security policy.



Configuring Gateways to inspect outbound and inbound HTTPS

This section gives an example of how to configure a Gateways to inspect outbound and inbound HTTPS traffic.

Workflow overview

1. Enable HTTPS Inspection on the Security Gateway.
2. Configure the Security Gateway to use the certificate.
 - Outbound Inspection - Generate a new certificate for the Security Gateway.
 - Inbound Inspection - Import the certificate for the internal server.
3. Configure the HTTPS Inspection Rule Base.
4. Install the Access Control Policy.

Enabling HTTPS Inspection

You must enable HTTPS inspection on each Security Gateway.

To enable HTTPS Inspection on a Security Gateway:

1. From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2. Click **HTTPS Inspection > Step 3**.
3. Select **Enable HTTPS Inspection**.

The first time you enable HTTPS inspection on one of the Security Gateways, you must create an outbound CA certificate for HTTPS inspection or import a CA certificate already deployed in your organization. This outbound certificate is used by all Security Gateways managed on the Security Management Server.

Creating an Outbound CA Certificate

The outbound CA certificate is saved with a P12 file extension and uses a password to encrypt the private key of the file. The Security Gateways use this password to sign certificates for the sites accessed. You must keep the password because it is also used by other Security Management Servers that import the CA certificate to decrypt the file.

After you create an outbound CA certificate, you must export it so it can be distributed to clients. If you do not deploy the generated outbound CA certificate on clients, users will receive SSL error messages in their browsers when connecting to HTTPS sites. You can configure a troubleshooting option that logs such connections.

After you create the outbound CA certificate, a certificate object named Outbound Certificate is created. Use this object in rules that inspect outbound HTTPS traffic in the HTTPS inspection Rule Base.

To create an outbound CA certificate:

1. In SmartConsole Gateways & Servers view, right-click the Security Gateway object and select **Edit**.
The **Gateway Properties** window opens.
2. In the navigation tree, select **HTTPS Inspection**.
3. In **Step 1** of the **HTTPS Inspection** page, click **Create**.
The **Create** window opens.
4. Enter the necessary information:
 - **Issued by (DN)** - Enter the domain name of your organization.
 - **Private key password** - Enter the password that is used to encrypt the private key of the CA certificate.
 - **Retype private key password** - Retype the password.
 - **Valid from** - Select the date range for which the CA certificate is valid.
5. Click **OK**.
6. Export and deploy the CA certificate ("[Exporting and Deploying the Generated CA](#)" on page 121).

Importing an Outbound CA Certificate

You can import a CA certificate that is already deployed in your organization or import a CA certificate created on one Security Management Server to use on another Security Management Server.

Best Practice - Use *private* CA Certificates.

For each Security Management Server that has Security Gateways enabled with HTTPS inspection, you must:

- Import the CA certificate.
- Enter the password the Security Management Server uses to decrypt the CA certificate file and sign the certificates for users. Use this password only when you import the certificate to a new Security Management Server.

To import a CA certificate:

1. If the CA certificate was created on another Security Management Server, export the certificate from the Security Management Server on which it was created ("[Exporting a Certificate from the Security Management Server](#)" on page 120).
2. In the SmartConsole **Gateways & Servers** view, right-click the Security Gateway object and select **Edit**.

The **Gateway Properties** window opens.

3. In the navigation tree, select **HTTPS Inspection**.
4. In **Step 1** of the **HTTPS Inspection** page, click **Import**.

The **Import Outbound Certificate** window opens.

5. Browse to the certificate file.
6. Enter the **private key password**.
7. Click **OK**.
8. If the CA certificate was created on another Security Management Server, deploy it to clients ("[Exporting and Deploying the Generated CA](#)" on page 121).

Exporting a Certificate from the Security Management Server

If you use more than one Security Management Server in your organization, you must *first* export the CA certificate with the `export_https_cert` CLI command from the Security Management Server on which it was created before you can import it to other Security Management Servers.

Command syntax:

```
export_https_cert [-local] | [-s server] [-f certificate file name under FWDIR/tmp] [-help]
```

To export the CA certificate:

On the Security Management Server, run this command:

```
$FWDIR/bin/export_https_cert -local -f [certificate file name under FWDIR/tmp]
```

Example

```
$FWDIR/bin/export_https_cert -local -f mycompany.p12
```

Exporting and Deploying the Generated CA

To prevent users from getting warnings about the generated CA certificates that HTTPS inspection uses, install the generated CA certificate used by HTTPS inspection as a trusted CA. You can distribute the CA with different distribution mechanisms such as Windows GPO. This adds the generated CA to the trusted root certificates repository on client computers.

When users run standard updates, the generated CA will be in the CA list and they will not receive browser certificate warnings.

To distribute a certificate with a GPO:

1. From the **HTTPS Inspection** window of the Security Gateway, click **Export certificate**.
2. Save the CA certificate file.
3. Use the Group Policy Management Console ("**Deploying Certificates by Using Group Policy**" on page 121) to add the certificate to the Trusted Root Certification Authorities certificate store.
4. Push the Policy to the client computers in the organization.
Note - Make sure that the CA certificate is pushed to the client computer organizational unit.
5. Test the distribution by browsing to an HTTPS site from one of the clients and verifying that the CA certificate shows the name you entered for the CA certificate that you created in the **Issued by** field.

Deploying Certificates by Using Group Policy

You can use this procedure to deploy a certificate to multiple client machines with Active Directory Domain Services and a Group Policy Object (GPO). A GPO can contain multiple configuration options, and is applied to all computers in the scope of the GPO.

Membership in the local Administrators group, or equivalent, is necessary to complete this procedure.

To deploy a certificate using Group Policy:

1. On the Microsoft Windows Server, open the **Group Policy Management Console**.
2. Find an existing GPO or create a new GPO to contain the certificate settings. Make sure the GPO is associated with the domain, site, or organization unit whose users you want affected by the policy.
3. Right-click the GPO and select **Edit**.
The **Group Policy Management Editor** opens and shows the contents of the policy object.
4. Open **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Publishers**.
5. Click **Action > Import**.
6. Do the instructions in the **Certificate Import Wizard** to find and import the certificate you exported from SmartConsole.
7. In the navigation pane, click **Trusted Root Certification Authorities** and repeat steps 5-6 to install a copy of the certificate to that store.

Configuring Inbound HTTPS Inspection

Configure the Security Gateway for inbound HTTPS Inspection.

To enable inbound HTTPS traffic inspection:

1. From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2. Click **HTTPS Inspection > Step 3**.
3. Select **Enable HTTPS Inspection**.
4. Import server certificates for servers behind the organization Security Gateways ("[Assigning a Server Certificate for Inbound HTTPS Inspection](#)" on page 122).
5. Define an HTTPS inspection policy:
 - Create rules
 - Add a server certificate to the **Certificate** column of each rule.

Assigning a Server Certificate for Inbound HTTPS Inspection

Add the server certificates to the Security Gateway. This creates a server certificate object

When a client from outside the organization initiates an HTTPS connection to an internal server, the Security Gateway intercepts the traffic. The Security Gateway inspects the inbound traffic and creates a new HTTPS connection from the gateway to the internal server. To allow HTTPS inspection, the Security Gateway must use the original server certificate and private key. The Security Gateway uses this certificate and the private key for SSL connections to the internal servers.

After you import a server certificate (with a P12 file extension) to the Security Gateway, add the object to the HTTPS Inspection Policy.

Do this procedure for all servers that receive connection requests from clients outside of the organization.

To add a server certificate for inbound HTTPS inspection:

1. In SmartConsole, go to **Security Policies > Shared Policies > HTTPS Inspection**.
2. Click **Open HTTPS Inspection Policy In SmartDashboard**.
SmartDashboard opens.
3. Click **Server Certificates**.
4. Click **Add**.
The **Import Inbound Certificate** window opens.
5. Enter a **Certificate name** and a **Description** (optional).
6. Browse to the certificate file.
7. Enter the **Private key password**. Enter the same password that was used to protect the private key of the certificate on the server.
8. Click **OK**.

The **Successful Import** window opens the first time you import a server certificate. It shows you where to add the object in the HTTPS Inspection Rule Base. Click **Don't show this again** if you do not want to see the window each time you import a server certificate and **Close**.

HTTPS Inspection Policy

The HTTPS Inspection rules define how the Security Gateways inspect HTTPS traffic. The HTTPS Inspection rules can use the URL Filtering categories to identify traffic for different websites and applications. For example, to protect the privacy of your users, you can use a rule to ignore HTTPS traffic to banks and financial institutions.

The HTTPS Inspection rules are applied to all the Software Blades that have HTTPS Inspection enabled. These are the Software Blades that support HTTPS Inspection:

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

To open the HTTP Inspection Policy

1. In SmartConsole, go to **Security Policies > Shared Policies > HTTPS Inspection**.
2. Click **Open HTTPS Inspection Policy In SmartDashboard**.

HTTPS Inspection rules in SmartDashboard

These are the fields that manage the rules for the HTTPS Inspection security policy.

Field	Description
No.	Rule number in the HTTPS Inspection Rule Base.
Name	Name that the system administrator gives this rule.
Source	Network object that defines where the traffic starts.
Destination	Network object that defines the destination of the traffic.
Services	The network services that are inspected or bypassed. By default, the services HTTPS on port 443 and HTTP_and_HTTPS proxy on port 8080 are inspected. You can add or delete services from the list.
Site Category	Categories for applications or web sites that are inspected or bypassed.
Action	Action that is done when HTTPS traffic matches the rule. The traffic is inspected or ignored (Bypass).
Track	Tracking and logging action that is done when traffic matches the rule.
Install On	Network objects that will get the HTTPS Inspection rule. You can only select Security Gateways that have HTTPS Inspection enabled.

Field	Description
Certificate	The certificate that is used for this rule. - Inbound HTTPS inspection - Select the certificate that the internal server uses. - Outbound HTTPS inspection - Select the Outbound Certificate object that you are using for the computers in the network. When there is a match to a rule, the Security Gateway uses the selected server certificate to communicate with the source client. You can create server certificates from HTTPS Inspection > Server Certificates > Add.
Comment	An optional field that lets you summarize the rule.

Configuring HTTPS Inspection Rules

Create different HTTPS Inspection rules for outbound and inbound traffic.

The outbound rules use the certificate that was generated for the Security Gateway.

The inbound rules use a different certificate for each internal server.

You can also create bypass rules for traffic that is sensitive and is not inspected. Make sure that the bypass rules are at the top of the HTTPS Inspection Rule Base.

After creating the rules, install the Access Control Policy.

Sample HTTPS Inspection Rule Base

This table shows a sample HTTPS Inspection Rule Base for a typical policy. (The **Track** and **Install On** columns are not shown. **Track** is set to **None** and **Install On** is set to **Any**.)

No	Name	Source	Destination	Services	Site Category	Action	Blade	Certificate
1	Inbound traffic	Any	WebCalendar Server	HTTPS	Any	Inspect	Any	WebCalendarServer CA
2	Financial sites	Any	Internet	HTTPS HTTP_HTTPS_proxy	Financial Services	Bypass	Any	Outbound CA
3	Outbound traffic	Any	Internet	HTTPS HTTP_HTTPS_proxy	Any	Inspect	Any	Outbound CA

- Inbound traffic** - Inspects HTTPS traffic to the network object WebCalendarServer. This rule uses the WebCalendarServer certificate.
- Financial sites** - This is a bypass rule that does not inspect HTTPS traffic to websites that are defined in the Financial Services category. This rule uses the Outbound CA certificate.
- Outbound traffic** - Inspects HTTPS traffic to the Internet. This rule uses the Outbound CA certificate.

Bypassing HTTPS Inspection for Software Update Services

Check Point dynamically updates a list of approved domain names of services from which content is always allowed. This option makes sure that Check Point updates or other 3rd party software updates are not blocked. For example, updates from Microsoft, Java, and Adobe.

To bypass HTTPS inspection for software updates:

1. In SmartConsole, go **Manage & Settings > Blades > HTTPS Inspection > Configure In SmartDashboard**.
2. In SmartDashboard, click the **HTTPS Inspection** tab.
3. Click **Policy**.
4. In the Policy pane, select **Bypass HTTPS Inspection of traffic to well known software update services (list is dynamically updated)**. This option is selected by default.
5. Click **list** to see the list of approved domain names.

Managing Certificates by Gateway

The **Gateways** pane lists the gateways with HTTPS Inspection enabled. Select a gateway and click **Edit** to edit the gateway properties.

In the CA Certificate section, you can **renew** the certificate validity date range if necessary and **export** it for distribution to the organization client machines.

If the Security Management Server which manages the selected Security Gateway does not have a generated CA certificate installed on it, you can add it with **Import certificate from file**.

- You can import a CA certificate already deployed in your organization.
- You can import a CA certificate from another Security Management Server. Before you can import it, you must first export ("[Exporting a Certificate from the Security Management Server](#)" on page 120) it from the Security Management Server on which it was created.

Adding Trusted CAs for Outbound HTTPS Inspection

When a client initiates an HTTPS connection to a web site server, the Security Gateway intercepts the connection. The Security Gateway inspects the traffic and creates a new HTTPS connection from the Security Gateway to the designated server.

When the Security Gateway establishes a secure connection (an SSL tunnel) to the designated web site, it must validate the site server certificate.

HTTPS Inspection comes with a preconfigured list of trusted CAs. This list is updated by Check Point when necessary and is automatically downloaded to the Security Gateway. The system is configured by default to notify you when a Trusted CA update file is ready for installation. The notification in SmartDashboard shows as a pop-up notification or in the **Trusted CAs** window in the **Automatic Updates** section. After you install the update, make sure to install the policy. You can select to disable the automatic update option and manually update the Trusted CA list.

If the Security Gateway receives a non-trusted server certificate from a site, by default the user gets a self-signed certificate and not the generated certificate. A page notifies the user that there is a problem with the website security certificate, but lets the user continue to the website.

You can change the default setting to block untrusted server certificates.

Saving a CA Certificate

You can save a selected certificate in the trusted CAs list to the local file system.

To export a CA certificate:

1. In SmartDashboard, open **HTTPS Inspection > Trusted CAs**.
2. Click **Actions > Export to file**.

3. Browse to a location, enter a file name and click **Save**.

A CER file is created.

HTTPS Validation

In the **HTTPS Validation** page of SmartDashboard you can set options for

- Fail mode
- HTTPS site categorization mode
- Server validation.
- Certificate blacklisting
- Troubleshooting

To learn more about these options, see the Help. Click **?** in the **HTTPS Validation** page.

Showing HTTPS Inspection Logs

The predefined log query for HTTPS Inspection shows all HTTPS traffic that matched the HTTPS Inspection policy, and was configured to be logged.

To see HTTPS Inspection Logs:

1. In the SmartConsole **Logs & Monitor > Logs** tab, click **Favorites**.
2. Select the **HTTPS Inspection** query.

The logs includes an **HTTP Inspection Action** field. The field value can be *inspect* or *bypass*. If HTTPS Inspection was not done on the traffic, this field does not show in the log.

Configuring the Geo Policy

The Geo Policy lets you control network traffic for specified countries. An IP-to-country database maps IP addresses to countries. You can configure different Geo policies that block or allow traffic for different countries. Private IP addresses are allowed unless the connection is explicitly blocked. Check Point control connections (such as between Security Gateways and the Security Management Server) are always allowed, regardless of the Geo policy.

Follow this workflow to configure a Geo Policy:

1. Create a Geo Policy.
2. Configure exceptions to the policy (optional).
3. Apply the new Geo Policy to target Security Gateways.
4. Publish the configuration changes and install the Access Control Policy.

To create a new Geo Policy:

1. In SmartConsole, go to the **Security Policies** page.
2. In the **Shared Policies** section, click **Geo Policy**.
3. From the drop-down **Edited Policy** menu, select **New**.
4. In the Object Name window that opens, enter a name for the new Geo Policy.
5. Click **OK**.

6. Select an **Activation Mode**:
 - **Active** - Policy is enabled
 - **Monitory Only** - Traffic that matches the policy is allowed and logged
 - **Inactive** - Policy is disabled
7. In Policy for specific countries section, click the plus sign.
The **Geo Policy - Add new rule** window opens.
8. Configure the **Rule Settings**:
 - **Country** - Select or search for a country on the list
 - **Action** - Select **Accept** to allow the traffic or **Drop** to reject it
 - **Direction** - **From and To Country** for bidirectional traffic, or **To Country** or **From Country** for traffic only in a specific direction
 - **Track** - Select to Log, send Alerts, send Mail, send SNMP Traps, or to send one of possible three custom User Alerts (you can also choose to not do any tracking)
 - **Comment** - optional comment
9. Set the default **Action** and **Track** option for the **Policy for other countries**.
10. Optional - Select **Aggregate logs by country**.
11. Publish the Session to save the configuration changes.

To configure exceptions to a Geo Policy:

1. In the **Shared Policies** section of the **Security Policies** page, click **Exceptions**.
2. Click **New**.
The **New Exception Rule** window opens.
3. In the **Apply to** section, select the **Profile** to which you want to apply the exception.
4. In the **Source** and **Destination** sections, select the exception criteria:
 - **Network Object** - A specific internal host or a network (or **Any**)
 - **IP Address** - A specific IP address
5. Select a **Service** or specify a **TCP** or **UDP Port/Range**.
6. Select the target gateways for the exception to **Install On**.
7. Add an optional **Comment** and click **OK**.

To apply a Geo Policy:

1. In the **Shared Policies** section of the **Security Policies** page, click **Gateways**.
2. Select a gateway or a cluster of gateways and click **Edit**.
The gateway **Geo Policy** window opens.
3. From the Assign Policy drop-down list, select a Geo Policy.
4. Click **OK**.

You can also edit Geo Policies, or delete them (if they are not applied to any target gateways).

To delete a Geo Policy:

1. In the **Shared Policies** section of the **Security Policies** page, click **Gateways**.
2. From the **Edited Policy** drop-down list, select a policy.
The rules of the selected Geo Policy show.
3. Click to open the **Edited Policy** list again, and select **Delete**.
4. Click **Yes** to confirm.
Note - If the policy is applied to a gateway or a cluster of gateways, the warning will show and the policy will not be deleted.

To edit a Geo Policy:

1. In the **Shared Policies** section of the **Security Policies** page, click **Gateways**.
2. From the **Edited Policy** drop-down list, select a policy.
The rules of the selected Geo Policy show.
3. Make changes to the policy.
4. Publish the changes and install the Access Control Policy.

Adding Users to the Policy

In This Section:

Using Identity Awareness.....	129
Using User Directory	134
To Learn More About Adding Users to the Policy.....	140

Using Identity Awareness

The Identity Awareness Software Blade lets you configure the Security Gateways to enforce access control for individual users and groups. You can use Identity Sources to get information about users and groups to add flexibility and security for the Rule Base. Identity Awareness lets you create rules in the Access Control and Threat Prevention Rule Bases.

Identity Sources

After the Security Gateway acquires the identity of a user, user-based rules can be enforced on the network traffic. Identity Awareness can use these sources to identify users:

- **Browser-Based Authentication** - Uses a Captive Portal to authenticate users. If Transparent Kerberos Authentication is configured, the browser attempts to transparently acquire users' identities using Kerberos tickets for users logged in to the domain, before redirecting users to the Captive Portal.
- **AD Query** - Get identity data from Microsoft Active Directory (AD) servers.
- **Identity Agent** - Client that is installed on endpoint computers connects to a Security Gateway and authenticates users.
- **Terminal Servers** - A Terminal Server Identity Agent is used to identify individual user traffic coming from terminal servers. This is used in environments with application servers that host Microsoft Terminal Servers, Citrix XenApp, and Citrix XenDesktop.
- **RADIUS Accounting** - You can configure a Security Gateway with Identity Awareness to use **RADIUS Accounting** to get user and computer identities directly from a RADIUS accounting client. Identity Awareness uses this information to apply access permissions to the connection.
- **Identity Collector** - Identity Collector is a Windows-based application which collects information about identities and their associated IP addresses and sends it to Check Point firewalls for identity enforcement. Identity Collector supports these sources:
 - Microsoft Active Directory Domain Controllers
 - Cisco Identity Services Engine (ISE) Servers, versions 1.3 and 2.0The Identity Collector can connect with more than one Identity Source at a time. The Identity Sources are organized in Query Pools. The Identity Collector sends the Identity Server information from the Identity Sources selected in the Query Pool assigned to the gateway.
- **Identity Web API** - The Identity Web API gives you a flexible method for creating identities. With the Identity Awareness Web API, you can:
 - Create and revoke identities
 - Query the Identity Awareness Software Blade regarding users, IPs, and computers.

- **Remote Access** - Identities are acquired for Mobile Access clients and IPSec VPN clients configured to work in Office Mode when they connect to the Security Gateway. This option is enabled by default.

If there is more than one Security Gateway enabled with Identity Awareness that share identities with each other and have Office Mode configured, each gateway must be configured with different office mode ranges.

Browser-Based Authentication

Browser-Based Authentication uses the Internet browser to identify users. You can use these Browser-Based Authentication solutions:

- Captive Portal
- Transparent Kerberos Authentication

Captive Portal uses a web interface to authenticate users before they can access network resources. When users try to access a protected resource, they must log in to a web page to continue.

When Transparent Kerberos Authentication is enabled, the Transparent Authentication page tries to authenticate users before the Captive Portal web page opens. The Transparent Authentication page communicates with the AD to use the Kerberos protocol to authenticate the users. If the users are successfully authenticated, then they can access the network resources. If they are not authenticated, then they are redirected to the Captive Portal.

AD Query

The Security Gateway registers to receive security event logs from the AD domain controllers when the security policy is installed. When a user authenticates with AD credentials, these event logs are generated and are sent to the Security Gateway. The gateway identifies the user based on the AD security event log, and enforces the appropriate Identity Awareness rule to the traffic that this user sends.

Enabling Identity Awareness

There is an Identity Awareness configuration wizard in SmartConsole that helps you enable and configure the Identity Awareness Software Blade. You can use the configuration wizard on these identity sources:

- AD Query
- Browser-Based Authentication
- Terminal Servers

Using the Identity Awareness Configuration Wizard

Use the Identity Awareness Configuration wizard to configure how the Security Gateway gets information about users and computers. The wizard automatically creates an Account Unit ("[Account Units](#)" on page [135](#)).

This is an example of how to configure the AD query and browser-based methods for Identity Awareness.

To use the Identity Awareness configuration wizard:

1. In SmartConsole, go to the **Gateways & Servers** page and double-click the Security Gateway object.
The gateway properties window opens.
2. From the navigation tree, click **General Properties**.
3. From the **Network Security** tab, select **Identity Awareness**.
The **Identity Awareness Configuration** wizard opens.
4. Select **AD Query** and **Browser-Based Authentication** and then click **Next**.
The **Integration With Active Directory** window opens.
5. Select the AD domain and enter the **Username** and the **Password**.
Make sure that the AD account has domain administrator privileges. Alternatively, you can let non-administrators make AD connections
<http://supportcontent.checkpoint.com/solutions?id=sk93938>.
Note - you can also select **Create new domain** and configure a new AD (Active Directory) Account Unit object.
6. Click **Connect**.
The message about user credentials shows.
7. Click **Next**.
The **Browser-Based Authentication Settings** window opens.
8. Enter the URL for the Captive Portal and then click **Next**.
The **Identity Awareness is Now Active** window opens.
9. Click **Finish**.
10. Install the policy.

Identity Awareness and Remote Access

Identity Awareness for Mobile Access and IPsec VPN clients works in Office Mode for Security Gateways. The Remote Access option is included as an identity source when you enable Identity Awareness.

To enable or disable Remote Access for Identity Awareness:

1. In SmartConsole, go to the **Gateways & Servers** page and double-click the Security Gateway object.
The gateway properties window opens.
2. From the navigation tree, click **Identity Awareness**.
3. Select or clear **Remote Access**.
4. Click **OK**.
5. Install the policy.

Working with Access Roles

After you enable Identity Awareness, you create Access Role objects.

You can use Access Role objects as source and/or destination parameter in a rule. Access Role objects can include one or more of these objects:

- Networks
- Users and user groups
- Computers and computer groups
- Remote Access Clients

To create an Access Role object:

1. In SmartConsole, open the **Object Explorer** (Ctrl+E).
2. Click **New > Users > Access Role**.
The **New Access Role** window opens.
3. Enter a **Name** and **Comment** (optional).
4. On the **Networks** page, select one of these:
 - **Any network**
 - **Specific networks** - Click the plus sign and select a network - click the plus sign next to the network name or search for a known network
5. On the **Users** page, select one of these:
 - **Any user**
 - **All identified users** - Includes users identified by a supported authentication method.
 - **Specific users** - Click the plus sign and select a user - click the plus sign next to the username or search for a known user or user group.
6. On the **Machines** page, select one of these:
 - **Any machine**
 - **All identified machines** - Includes computers identified by a supported authentication method
 - **Specific machines** - Click the plus sign and select a device - click the plus sign next to the device name or search for a known device or group of devices

For computers that use Full Identity Agents, you can select (optional) **Enforce IP Spoofing protection**.
7. On the **Remote Access Clients** page, select the **Allowed Clients** or add new ones. For R77.xx Gateways or lower, you must choose **Any**.
8. Click **OK**.

Using Identity Awareness in the Access Control Policy

The Identity Awareness Software Blade lets you configure your Access Control Policy to allow connections for users regardless of what computer they are using. Use **Access Role** objects in the **Source** column of a rule, and Identity Awareness Software Blade will identify users based on those objects. You can also configure the **Accept** action to redirect traffic from an unidentified user to a Captive Portal.

Sample gateway workflow with Identity Awareness

The gateway inspects traffic that starts from a source that matches the **Access Role** object and tries to identify the user.

- If the user is identified, the traffic is allowed.
- If the user is not identified, the traffic is only allowed when the user authenticates to the Captive Portal. If Captive Portal is not enabled, or the user does not authenticate, then the traffic is dropped.

Adding an Access Role to a Rule

You can add rules with Access Role objects as the **Source** or **Destination** to the Access Control policy for Security Gateways that have the Identity Awareness Software Blade enabled.



Note - Rules that use Access Role objects cannot be enforced on Security Gateways that do not have Identity Awareness enabled.

To add an Access Role object to a rule:

1. Select a policy from the **Access Control > Policy** tree.
2. Click the plus sign in the **Source** or the **Destination** cell of a rule.
3. In the window that opens, click the **Filter** button and select **Categories > Users > Access Roles**.
4. Click the plus sign for every Access Role object you want to add.
5. Install the policy.

Redirecting to a Captive Portal

You can configure rules that use **Access Role** objects and the **Accept** action with the **Action Settings** option, to redirect HTTP traffic to a Captive Portal. The rule allows traffic when the users that match the source **Access Role** object are identified. If the **Enable Identity Captive Portal** option is enabled, the gateway identifies users this way:

1. The Identity Awareness source identifies the user
2. The user authenticates at the Captive Portal

Rules can redirect HTTP traffic according to these parameters:

- **Source** - Includes an **Access Role** object
- **Action** - Uses **Accept**

To enable Captive Portal for a rule:

1. Right-click the **Action** cell and select **More**.
The **Action Settings** window opens.
2. Select **Enable Identity Captive Portal**.
3. Click **OK**.
The **Action** column shows **accept (display captive portal)**.
4. Install the policy.

Sample Identity Awareness Rules

This table shows sample Identity Awareness rules for a Firewall Rule Base. (The **VPN**, **Track** and **Time** columns are not shown. **Track** is set to **Log**, and **VPN** and **Time** are set to **Any**.)

No.	Name	Source	Destination	Service	Action
1	CEO allow	John_Smith_CEO	Any	Any	Accept Display Captive Portal
2	HR server allow	HR_Partners	HR_Server	Any	Accept Display Captive Portal
3	Drop non-identified HR traffic	Any	HR_Server	Any	Drop
4	Internet access	Guests All_Domain_Users	Internet_proxy	HTTP and HTTPS proxy	Accept Display Captive Portal

1. **CEO allow** - Allows the CEO, John Smith, to access all the network resources. The CEO is identified by Identity Awareness AD Query or he authenticates to the Captive Portal.
2. **HR server allow** - Allows users that are defined in the HR_Partners **Access Role** object to access the HR_Server subnet. The HR users are identified by Identity Awareness AD Query or they authenticate to the Captive Portal.
3. **Drop non-identified HR traffic** - Drops all traffic to the HR_Server subnet. All authenticated users were allowed by the earlier rules.
4. **Internet access** - Allows HTTP and HTTPS traffic from the Guests and All_Domain_Users **Access Role** objects to the Internet. Domain users are identified by Identity Awareness or they authenticate to the Captive Portal. Guests authenticate to the Captive Portal.

Using User Directory

User Directory lets you integrate LDAP and other external user management servers with Check Point products and security solutions. These are some of the Software Blades that work with User Directory:

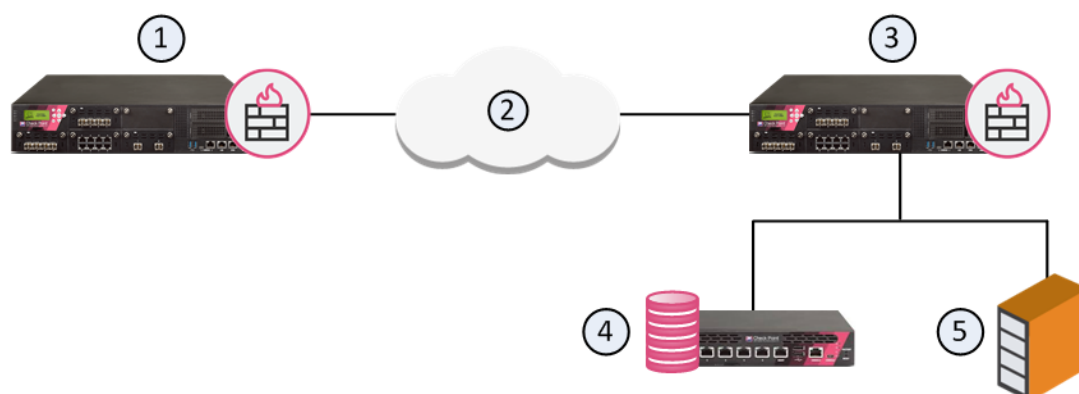
- Mobile Access
- Identity Awareness
- Data Loss Prevention

User Directory Features

- Use LDAP servers to manage user information for the network
- Security Gateways can retrieve CRLs (Certificate Revocation Lists)
- Security Management Server can use LDAP information to authenticate users
- High Availability can duplicate and backup user information across multiple LDAP servers
- Create multiple Account Units to work with distributed databases
- Use profiles to support multiple LDAP vendors
- Encrypt User Directory connections

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

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 137) - Configure how the Security Management Server uses the Account Unit
 - **Servers** ("**Configuring an LDAP Server**" on page 137) - Manage LDAP servers that are used by this Account Unit
 - **Objects Management** ("**Objects Management Tab**" on page 138) - Configure the LDAP server for the Security Management Server to query and the branches to use
 - **Authentication** ("**Authentication Tab**" on page 138) - 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 137) - Configure how the Security Management Server uses the Account Unit
 - **Servers** ("**Configuring an LDAP Server**" on page 137) - Manage LDAP servers that are used by this Account Unit
 - **Objects Management** ("**Objects Management Tab**" on page 138) - Configure the LDAP server for the Security Management Server to query and the branches to use
 - **Authentication** ("**Authentication Tab**" on page 138) - 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

Enabling User Directory

Configure SmartConsole to enable the Security Management Server to manage users in the Account Unit. 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**.
The **Global Properties** window opens.
2. In the **User Directory** view, select **Use User Directory for Security Gateways**.
3. Configure other login and password settings.
4. Click **OK**.
5. Make sure that the User Directory Software Blade is enabled:
 - a) In SmartConsole, open the **Object Explorer** (Ctrl+E).
 - b) Go to **Network Objects > Gateways and Servers**.
 - c) Double-click the Security Management Server object.
The object properties window opens.
 - d) Make sure that in the **Management** tab of the **General Properties** view, **Network Policy Management** and **User Directory** are selected.
 - e) Click **OK**.
 - f) Click **Close**.
6. Install the policy.

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**.

To Learn More About Adding Users to the Policy

To learn more about adding users to the Policy, see these guides:

- *R80.10 Identity Awareness Administration Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54825>
- *R80.10 Security Management Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54842>. Search for *Managing User Accounts*.

Logging and Monitoring

In This Section:

Log Analysis	141
Views and Reports	145
To Learn More About Logging and Monitoring	153

Log Analysis

SmartConsole lets you transform log data into security intelligence. Search results are fast and immediately show the log records you need. The Security Gateways send logs to the Log Servers on the Security Management Server or on a dedicated server. Logs show on the SmartConsole **Logs & Monitor Logs** tab. You can:

- Quickly search through logs with simple Google-like searches.
- Select from many predefined search queries to find the applicable logs.
- Create your own queries using a powerful query language.
- Monitor logs from administrator activity and connections in real-time.

Configuring Logging

To configure logging from a Security Gateway to a Security Management Server or a Log Server:

1. Define one or more Log Servers (if necessary).
2. Enable logging on the Security Management Server and the Log Servers.
3. Configure the Security Gateways to send logs to the Log Servers.
4. Install the Policy.

To enable logging on a server:

1. In SmartConsole, go to **Gateways & Servers** and double-click the server object.
The properties window opens.
2. Establish **Secure Internal Communication** between the Security Management Server and the Log Server. Make the certificate state: *Trust Established*.
3. In the **Management** tab, select **Logging & Status**.
4. From the navigation tree, click **Logs**.
This shows the Security Gateways that forward logs to this machine.
5. Make sure that **Enable Log Indexing** is selected. It is enabled by default optimizes the log search time.
6. Click **OK**.

To configure a Security Gateway to send logs to log servers:

1. In SmartConsole, go to **Gateways & Servers** and double-click the gateway object.
The gateway properties window opens.
2. From the navigation tree, click **Logs**.
3. In the **Send gateway logs and alerts to server** section, click the plus sign and select a server.
Make sure that in the **Type** column, **Send Logs and Alerts** is selected.
4. **Optional** - In the **In case one of the above log servers is unreachable, send logs to**, add backup servers.

To complete the configuration:

1. Click **Publish**.
2. Click **Install Policy**.

Enabling Log Indexing

Log indexing on the Security Management Server or Log Server reduces the time it takes to run a query on the logs. Log indexing is enabled by default.

In a standalone deployment, log indexing is disabled by default. Enable log indexing only if the standalone computer CPU has 4 or more cores.

To manually enable Log Indexing:

1. Open SmartConsole.
2. From the **Gateways & Servers** view, double-click the Security Management Server or Domain Log Server object.
The **General Properties** window opens.
3. In the **Management** tab, select **Logging & Status**.
4. From the navigation tree, click **Logs**.
5. Select **Enable Log Indexing**.
6. Click **OK**.
7. Click **Publish**.
8. From **Menu**, select **Install Database**.

Sample Log Analysis

This is a sample procedure that shows how to do an analysis of a log of a dropped connection.

To show a log of a dropped connection:

1. Log into SmartConsole.
2. Connect to the IP address of the Security Management Server, not to a Log Server.
3. In the **Security Policies > Access Control > Policy** view, select a rule with the **Drop** action.
4. In the bottom pane, click **Logs**.
This shows the logs for connections that were dropped by the Rule Base.
5. Double-click a log.
The **Log Details** window opens.

Tracking Options

Select these options in the **Track** column of a rule:

- **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. At a minimum, this is the Source, Destination, Source Port, and Destination Port. If there is a match on a rule that specifies an application, a session log shows the application name (for example, Dropbox). If there is a match on a rule that specifies a Data Type, the session log shows information about the files, and the contents of the files.
- **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.

Note - When upgrading from R77.xx or from R80 to R80.10, there are changes to the names of the options in the **Track** column. To learn more see sk116580

<http://supportcontent.checkpoint.com/solutions?id=sk116580>.

Advanced Track options

Detailed Log and **Extended Log** are only available if one or more of these Blades are enabled on the Layer: *Applications & URL Filtering*, *Content Awareness*, or *Mobile Access*.

- **Detailed Log** - Equivalent to the *Log* option, but also shows the application that matched the connections, even if the rule does not specify an application. **Best Practice** - Use for a cleanup rule (Any/Internet/Accept) of an Applications and URL Filtering Ordered Layer that was upgraded from an R77 Application Control Rule Base.
- **Extended Log** - Equivalent to the *Detailed* option, but also shows a full list of URLs and files in the connection or the session. The URLs and files show in the lower pane of the **Logs** view.

Log Generation

- **per Connection** - Select this to show a different log for each connection in the session. This is the default for rules in a Layer with only *Firewall* enabled. These are basic firewall logs.
- **per Session** - Select this to generate one log for all the connections in the same session ("**Log Sessions**" on page 144). This is the default for rules in a Layer with *Applications and URL Filtering* or *Content Awareness* enabled. These are basic Application Control logs.

Alert:

For each alert option, you can define a script in **Menu > Global Properties > Log and Alert > Alerts**.

- **None** - Do not generate an alert.
- **Alert** - Generate a log and run a command, such as: Show a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in the **Global Properties**.
- **SNMP** - Send an SNMP alert to the SNMP GUI, or run the script defined in the **Global Properties**.
- **Mail** - Send an email to the administrator, or run the mail alert script defined in the **Global Properties**.
- **User Defined Alert** - Send one of three possible customized alerts. The alerts are defined by the scripts specified in the **Global Properties**.

Log Sessions

A session is a user's activity at a specified site or with a specified application. The session starts when a *user* connects to an *application* or to a *site*. The Security Gateway includes all the activity that the user does in the session in one session log.

To search for log sessions:

In the **Logs** tab of the **Logs & Monitor** view, search for `type:Session`

To see details of the log session:

In the **Logs** tab of the **Logs & Monitor** view, select a session log.

In the bottom pane of the **Logs** tab, click the tabs to see details of the session log:

- **Connections** - Shows all the connections in the session. These show if **Per connection** is selected in the **Track** option of the rule.
- **URLs** - Shows all the URLs in the session. These show if **Extended Log** is selected in the **Track** option of the rule.
- **Files** - Shows all the files uploaded or downloaded in the session. These show if **Extended Log** is selected in the **Track** option of the rule, or if a Data Type was matched on the connection.

To see the session log for a connection that is part of a session:

1. In the **Logs** tab of the **Logs & Monitor** view, double-click on the log record of a connection that is part of a session.
2. In the **Log Details**, click the session icon  (in the top-right corner) to see the session log.

To configure the session timeout:

By default, after a session continues for three hours, the Security Gateway starts a new session log. You can change this in SmartConsole from the **Manage & Settings** view, in **Blades > Application Control and URL Filtering > Advanced Settings > General > Connection unification**.

For sessions that are blocked by the Access Control Policy, the Security Gateway starts a new session log after 30 seconds. A blocked session log include all the connections that are blocked in this period.

Views and Reports

In This Section:

- Catalog of Views and Reports 146
- Views..... 148
- Reports 151

You can create rich and customizable views and reports for log and event monitoring, that inform key stakeholders about security activities.

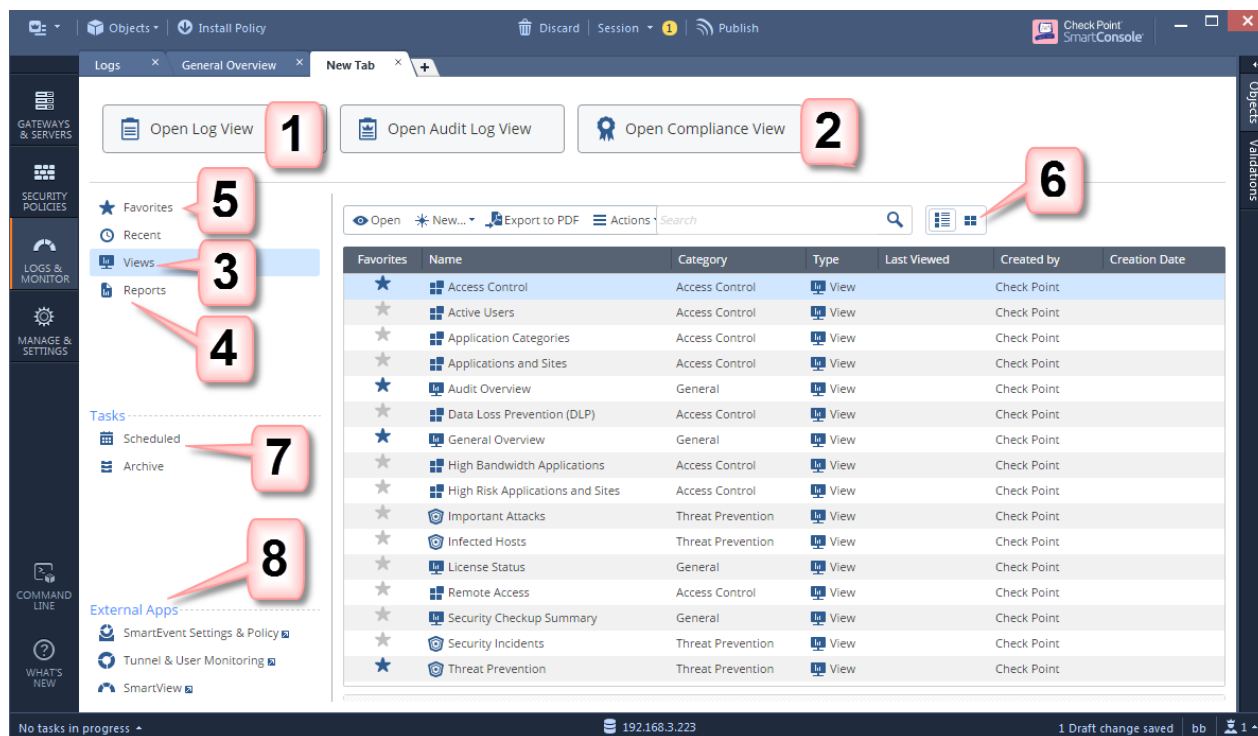
The views are available from two locations:

- **SmartConsole > Logs & Monitor.** Here you can also generate reports.
- **SmartView Web Application.** By browsing to: *https://<Server IP>/smartview/*
Where *Server IP* is IP address of the Security Management Server or SmartEvent server.

For a quick overview of Views and Reports in R80.10, see the online tutorial https://sc1.checkpoint.com/documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/html_frameset.htm.

Catalog of Views and Reports

In the Logs & Monitor view, click the (+) tab to open a catalog of all views and reports, predefined and customized. Click a view or report to open it.



Item	Description
1	Open Log View - See and search through the logs from all Log Servers. You can also search the logs from a Log Server that you choose. Open Audit Logs View - See and search records of actions done by SmartConsole administrators. These views come from the Log Servers. Other views come from the SmartEvent Server.
2	Compliance View - Optimize your security settings and ensure compliance with regulatory requirements.
3	Views - The list of predefined and customized views. A view is an interactive dashboard made up of widgets. The view tells administrators and other stakeholders about security and network events. Each widget is the output of a query. Widgets can show the information as a graph, table, or some other format. To find out more about the events, double-click a widget to drill down to a more specific view or raw log files.
4	Reports - The list of predefined and customized reports. A report has multiple views, and applies to the time that the report is generated. It gives more details than a view. There are several predefined reports, and you can create new reports. Reports can be customized, filtered, generated and scheduled. You cannot drill down into a report. A report is divided onto pages.
5	Favorites - Use this view to collect the views and reports you use the most.
6	Switch to Table View or Thumbnails View - The Table view is the default for views and reports. The Thumbnails view is the default for the Favorites and Recents.

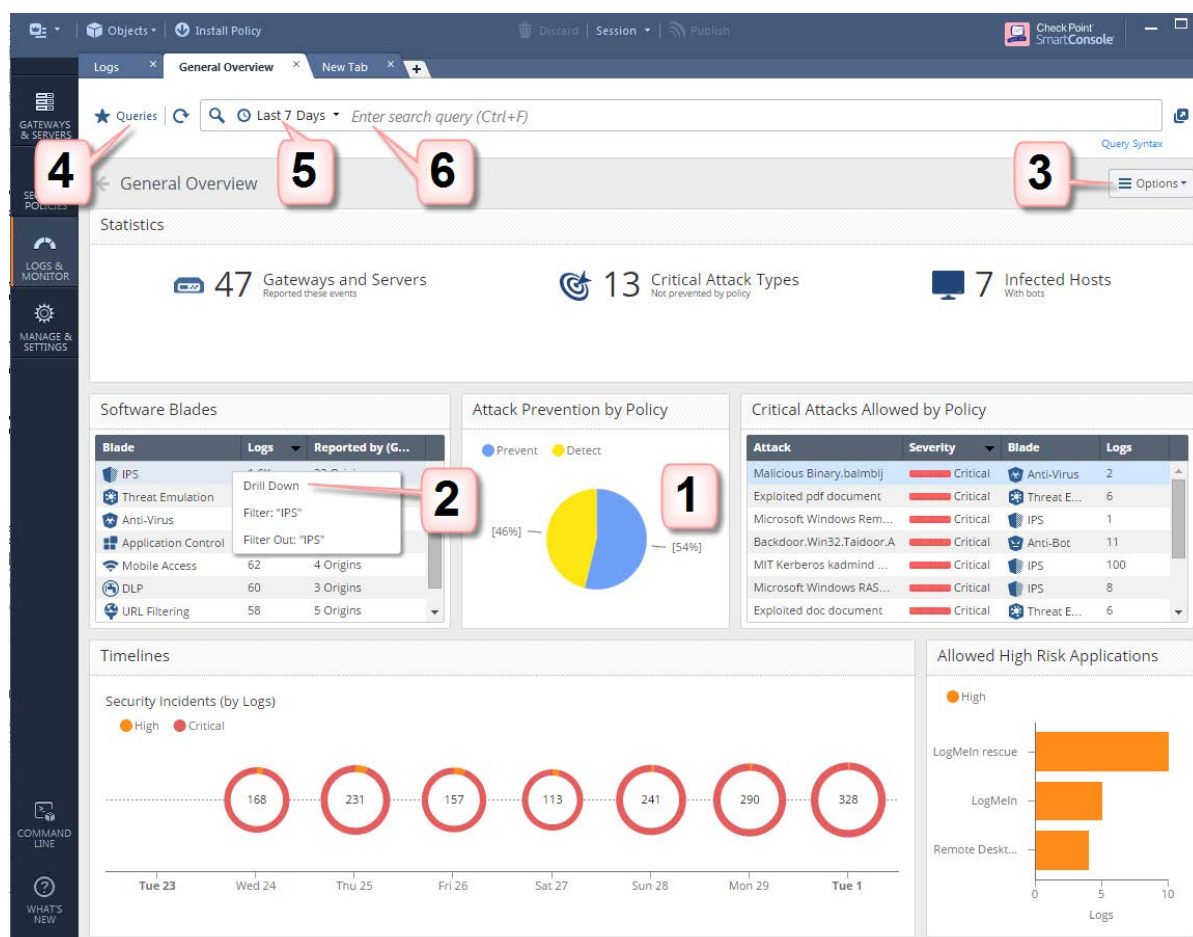
Item	Description
7	Scheduled Tasks - See and edit scheduled tasks. Archive - Completed and in-progress tasks for generating and exporting reports.
8	External Apps • SmartEvent Settings & Policy - The SmartEvent GUI client. Use it for initial setup and to define the SmartEvent Correlation Unit policy. The views in SmartConsole are a replacement for those in the SmartEvent GUI client. • Open Tunnel and User Monitoring - The SmartView Monitor GUI Client. The monitoring views in SmartConsole are a replacement for those in the SmartView Monitor GUI client, except for Tunnel and User Monitoring. • SmartView Web Application - A SmartEvent Web application that you can use to analyze events that occur in your environment. Use it to see an overview of the security information for your environment. It has the same real-time event monitoring and analysis views as SmartConsole, with the convenience of not having to install a client.

Views

Views tells administrators and other stakeholders about security and network events. A view is an interactive dashboard made up of widgets. Each widget is the output of a query. A Widget can show information in different formats, for example, a graph or a table.

SmartConsole comes with several predefined views. You can create new views that match your needs, or you can customize an existing view.

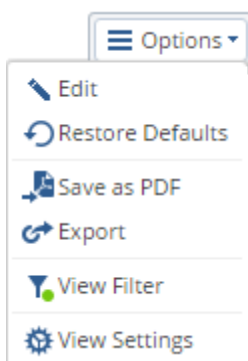
In the Logs & Monitor view, clicking the (+) tab opens a catalog of all views and reports, predefined and customized. Click a view to open it.



Item	Description
1	Widget - The output of a query. A Widget can show information in different formats, for example, a graph or a table.
2	Drill Down - To find out more about the events, double-click a widget to drill down to a more specific view or raw log files.
3	Options - Customize the view, restore defaults, Hide Identities, export.
4	Queries - Predefined and favorite search queries
5	Time Period - Specify the time periods for the view.
6	Query search bar - Define custom queries using the GUI tools, or manually entering query criteria. Shows the query definition for the most recent query.

Customization

Customize your views according to these options:



Click **Edit** to switch to view edit mode.

SmartConsole saves an administrator's customized views.

- To share a customized view with another administrator, use the Export and Import option ("Export and Import" on page 150).
- To customize a widget, see: Customizing Widgets

View Settings

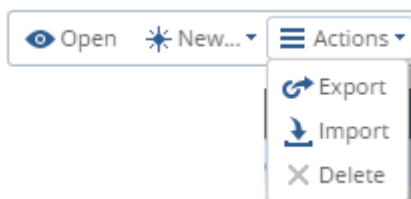
1. Enter a title.
2. To show more results, this option allows a table to spread across multiple pages when saved to PDF.

The **No page limit** option shows more results by spreading them across a number of pages.

Export and Import

To export the view layout and widget definitions to a file, use the **Export** option

To import the file from another server, or from another administrator, use the **Import** option in the Catalog (new tab).



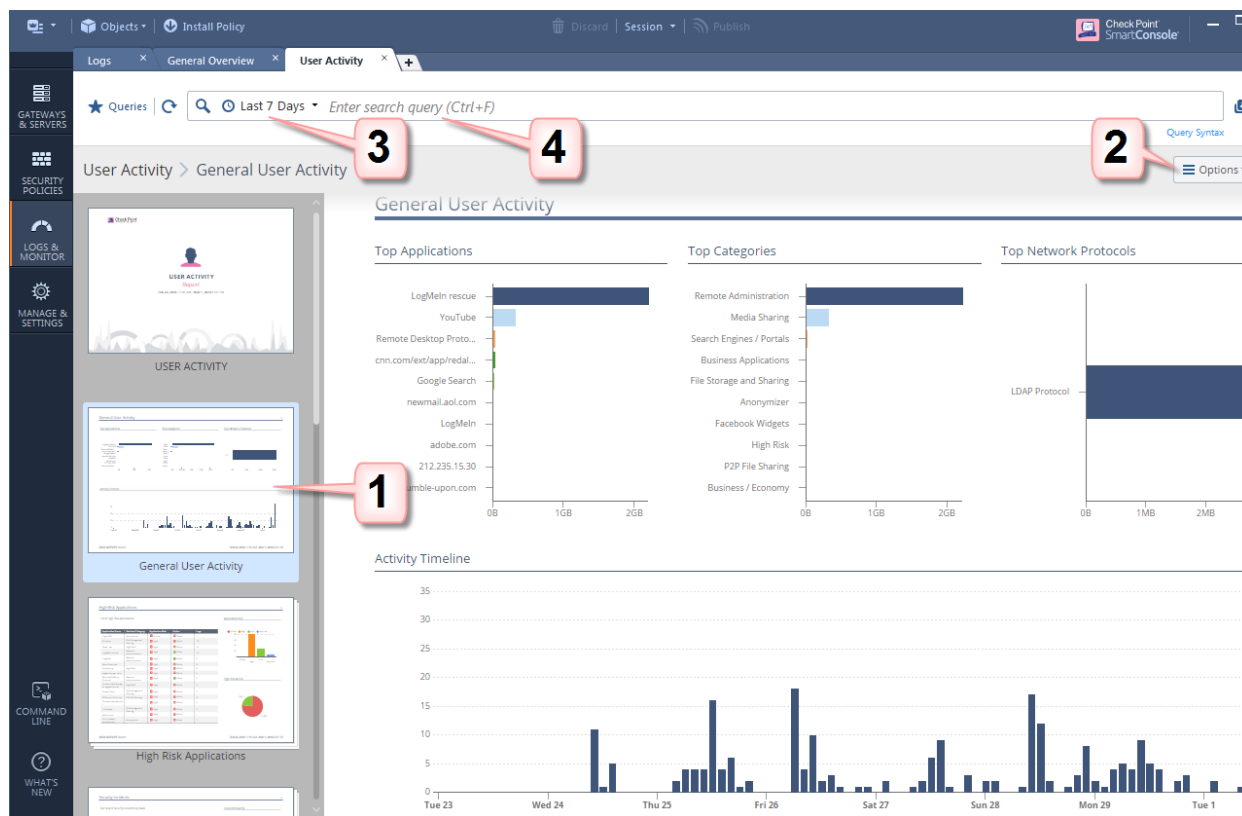
Save As PDF

The Save as PDF option saves the current view as a PDF file, based on the defined filters and time frame.

Reports

A report has multiple views, and applies to the time that the report is generated. It gives more details than a view. There are several predefined reports, and you can create new reports. Reports can be customized, filtered, generated and scheduled. You cannot drill down into a report.

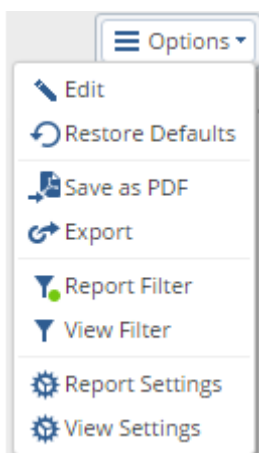
In the Logs & Monitor view, clicking the (+) tab opens a catalog of all views and reports, predefined and customized. Click a report to open it.



Item	Description
1	Preview bar - A report is divided onto pages, usually, one view on one page. Editing a report is done per page, in the same way as you edit a view.
2	Options - Customize, and generate a report.
3	Time Period - Specify the time periods for the report.
4	Query Search bar - Define custom queries using the GUI tools, or manually entering query criteria. Shows the query definition for the most recent query.

Customization

Customize your reports according to these options:



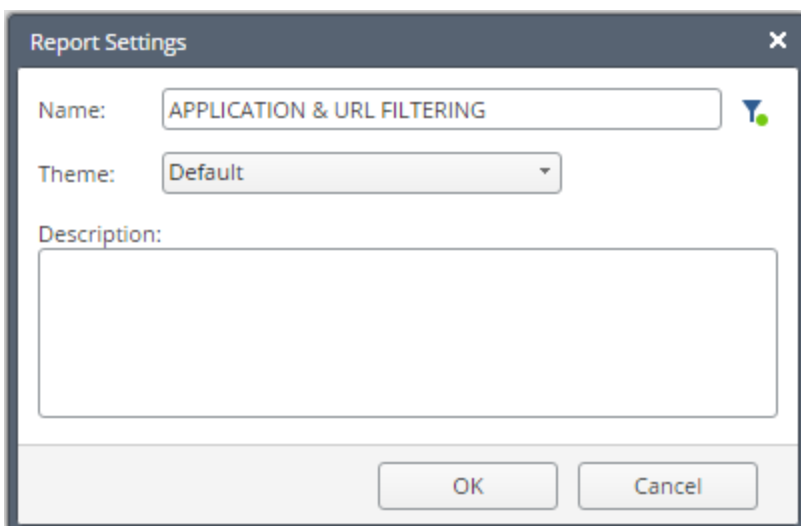
Click **Edit** to switch to the report edit mode.

To customize widgets, see: Customizing Widgets

SmartConsole saves an administrator's customized reports. To share customized reports with other administrators, use the **Export** and **Import** options.

Report Settings

Reports can be configured according to these options:



Customizing a Report

1. Select a report from the Catalog (new tab).
2. Click Options > **Edit**.
3. Select the page to edit.

You can also add or remove pages by clicking one of these:



4. Customize the widgets.
5. Add a widget, or arrange widgets in the view: Drag & Drop or expand.
6. Define filters.

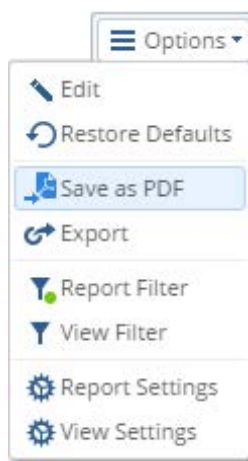
Note -

- Use the timeframe to see how the report will look.
- The timeframe and search bar are not saved with the report definition. Define them as needed when generating the report (**Save as PDF**).

See: Generating a Report (on page 153)

Generating a Report

1. Open the Catalog (new tab) and select a report.
2. Define the required timeframe and filter in the search bar.
3. Click **Options** > **Save As PDF**.

***Generating a Predefined Report in the SmartEvent GUI Client***

You can use predefined graphical report templates in the SmartEvent GUI for the most frequently seen security issues. Try these before you create a customized report.

Generate a predefined report in the SmartEvent GUI if you want to schedule it.

To generate a predefined report:

1. Open **SmartConsole** > **Logs & Monitor**.
2. Click the **+** to open a Catalog (new tab).
3. Click the **SmartEvent Settings & Policy** link.
4. In the SmartEvent GUI, open the **Reports** tab.
5. Select a **Default Report** for a Software Blade.
6. Click **Generate**.
7. In the **Generate a Report** window, select a time period.
8. Click **Generate**.

Your reports are saved in the **Report History**.

To Learn More About Logging and Monitoring

To learn more about logging and monitoring, see the *R80.10 Logging and Monitoring Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54830>.

Maximizing Network Performance and Redundancy

In This Section:

Solutions for Enhancing Network Performance and Redundancy	154
CoreXL	155
SecureXL	156
Multi-Queue	157
ClusterXL	158
VRRP Cluster	168
To Learn More About Maximizing Network Performance.....	174

Solutions for Enhancing Network Performance and Redundancy

These are features that you can enable to increase the performance of the Firewall:

- CoreXL
- SecureXL (Performance Pack)
- Multi-Queue

These Gateway clustering solutions enable you to enhance network redundancy:

- ClusterXL
- VRRP Cluster

These are software based features that are included in the Check Point operating systems. It is not necessary to purchase additional hardware to use them.

CoreXL

In a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated instance runs on one processing core. These instances handle traffic concurrently and each instance is a complete Firewall kernel that inspects traffic. When CoreXL is enabled, all Firewall instances in the Security Gateway process traffic through the same interfaces and apply the same gateway security policy.

When you enable CoreXL, the number of kernel instances is based on the total number of CPU cores.

Number of Cores	Number of Kernel Instances
1	1
2	2
4	3
6-20	Number of cores, minus 2
More than 20	Number of cores, minus 4. Up to a total of 40 instances. Cores can be IPv4 or IPv6.

Configuring CoreXL

Use the `cpconfig` command to open the wizard to enable CoreXL and configure the number of firewall instances.

To enable/disable CoreXL:

1. Log in to the Security Gateway.
2. Run `cpconfig`
3. Select **Configure Check Point CoreXL**.
4. Enable or disable CoreXL.
5. Reboot the Security Gateway.

To configure the number of instances:

1. Run `cpconfig`
2. Select **Configure Check Point CoreXL**.
3. If CoreXL is enabled, enter the number of firewall instances.
If CoreXL is disabled, enable CoreXL and then set the number of firewall instances.
4. Reboot the gateway.

To Learn More About CoreXL

To learn more about CoreXL, see the R80.10 *Performance Tuning Administration Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54765>

SecureXL

SecureXL is an acceleration solution that maximizes performance of the Firewall and does not compromise security. When SecureXL is enabled on a Security Gateway, some CPU intensive operations are processed by virtualized software instead of the Firewall kernel. The Firewall can inspect and process connections more efficiently and accelerate throughput and connection rates. These are the SecureXL traffic flows:

- **Slow path** - Packets and connections that are inspected by the Firewall and are not processed by SecureXL.
- **Accelerated path** - Packets and connections that are offloaded to SecureXL and are not processed by the Firewall.
- **Medium path** - Packets that require deeper inspection cannot use the accelerated path. It is not necessary for the Firewall to inspect these packets, they can be offloaded and do not use the slow path. For example, packets that are inspected by IPS cannot use the accelerated path and can be offloaded to the IPS PSL (Passive Streaming Library). SecureXL processes these packets more quickly than packets on the slow path.

The goal of a SecureXL configuration is to minimize the connections that are processed on the slow path.

Throughput Acceleration

Connections are identified by the 5 tuple attributes: source address, destination address, source port, destination port, protocol. When the packets in a connection match all the 5 tuple attributes, the traffic flow can be processed on the accelerated path.

The first packets of a new TCP connection require more processing and they are processed on the slow path. The other packets of the connection can be processed on the accelerated path and the Firewall throughput is dramatically increased.

Connection-rate Acceleration

SecureXL also improves the rate of new connections (connections per second) and the connection setup/teardown rate (sessions per second). To accelerate the rate of new connections, connections that do not match a specified 5 tuple are still processed by SecureXL.

For example, if the source port is masked and only the other 4 tuple attributes require a match. When a connection is processed on the accelerated path, SecureXL creates a template of that connection that does not include the source port tuple. A new connection that matches the other 4 tuples is processed on the accelerated path because it matches the template. The Firewall does not inspect the new connection and the Firewall connection rates are increased.

Configuring SecureXL

SecureXL is enabled by default. Configure it using the CLI.

To configure SecureXL:

1. Log in to the CLI on the Security Gateway.
2. Run `cpconfig`
3. Enter the option that enables or disables SecureXL.
For example, (9) Disable Check Point SecureXL
4. Enter `y` and then enter `11`.

**Note -**

- Run `fwaccel` or `fwaccel6` to dynamically enable or disable SecureXL acceleration for IPv4 or IPv6 traffic
- This setting does not survive reboot or the Security Gateway

To Learn More About SecureXL

To learn more about SecureXL, see the R80.10 *Performance Tuning Administration Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54765>

Multi-Queue

By default, the traffic for each interface is processed on one CPU core. If there are more CPU cores than interfaces, not all of the CPU cores are used to process traffic.

You can enable the Multi-Queue feature to assign more than one CPU core to one interface. Run the `cpmq` command to configure the Multi-Queue settings.

The SND (Secure Network Distributer) is part of SecureXL and CoreXL. It processes and helps to accelerate network traffic:

- SecureXL - Distributes traffic to the accelerated or slow path
- CoreXL - Processes traffic on a specified Firewall instance

Sample Multi-Queue Configuration

This sample configuration shows how CoreXL, SecureXL and Multi-Queue can help to use more CPU cores for SNDs to accelerate network traffic. There is a Security Gateway with two six core CPUs (total 12 CPU cores) and three interfaces:

- External
- Internal
- DMZ

	CPU cores for SND	CPU cores for CoreXL
Multi-Queue disabled	3	9
Multi-Queue enabled	6	6

To learn more about Multi-Queue, see the R80.10 *Performance Tuning Administration Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54765>

ClusterXL

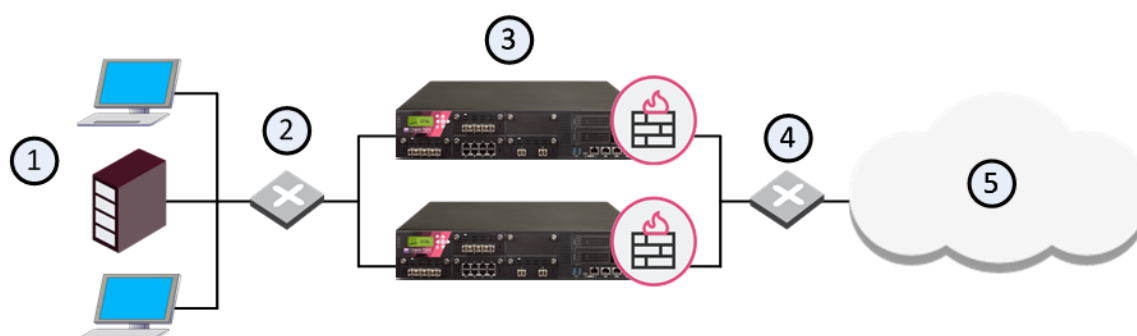
The Need for Clusters

Security Gateways and VPN connections are business critical devices. The failure of a Security Gateway or VPN connection can result in the loss of active connections and access to critical data. The Security Gateway between the organization and the world must remain open under all circumstances.

ClusterXL Solution

ClusterXL is a Check Point software-based cluster solution for Security Gateway redundancy and Load Sharing. A ClusterXL Security Cluster contains identical Check Point Security Gateways.

- A High Availability Security Cluster ensures Security Gateway and VPN connection redundancy by providing transparent failover to a backup Security Gateway in the event of failure.
- A Load Sharing Security Cluster provides reliability and also increases performance, as all members are active



Item	Description
1	Internal network
2	Switch for internal network
3	Security Gateways with ClusterXL Software Blade
4	Switch for external networks
5	Internet

IPv6 Support for ClusterXL

R80.10 ClusterXL supports High Availability clusters for IPv6. IPv6 status information is synchronized and the IPv6 clustering mechanism is activated during failover. However, IPv6 is not supported for Load Sharing clusters. Also, you cannot define IPv6 addresses for synchronization interfaces.

How ClusterXL Works

ClusterXL uses *State Synchronization* to keep active connections alive and prevent data loss when a member fails. With State Synchronization, each member "knows" about connections that go through other members.

ClusterXL uses virtual IP addresses for the cluster itself and unique physical IP and MAC addresses for the members. Virtual IP addresses do not belong to physical interfaces.

ClusterXL can work with OPSEC certified High Availability and Load Sharing products, which use the same State Synchronization infrastructure as Check Point ClusterXL.



Note - The *ClusterXL Administration Guide* contains information only for Security Gateway clusters. For information about the use of ClusterXL with VSX, see the *R80.10 VSX Administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54764>.

The Cluster Control Protocol

The Cluster Control Protocol (CCP) is the glue that links together the members in the Security Cluster. CCP traffic is distinct from ordinary network traffic and can be viewed using any network sniffer.

CCP runs on UDP port 8116, and has the following roles:

- It allows cluster members to report their own states and learn about the states of other members by sending keep-alive packets (this only applies to ClusterXL clusters).
- State Synchronization.

The Check Point CCP is used by all ClusterXL modes as well as by OPSEC clusters. However, the tasks performed by this protocol and the manner in which they are implemented may differ between cluster types.



Note - There is no need to add a rule to the Security Policy Rule Base that accepts CCP

Installation and Platform Support

ClusterXL must be installed in a distributed configuration in which the Security Management Server and the Security Cluster members are on different computers. ClusterXL is part of the standard Security Gateway installation.

For installation instructions, see the *R80.10 Installation and Upgrade Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54829>.

To see the ClusterXL supported platforms, see the *R80.10 Release Notes* <http://downloads.checkpoint.com/dc/download.htm?ID=54802>.

High Availability and Load Sharing in ClusterXL

ClusterXL is a software-based Load Sharing and High Availability solution that distributes network traffic between clusters of redundant Security Gateways.

ClusterXL has these High Availability features:

- Transparent failover in case of member failures
- Zero downtime for mission-critical environments (when using State Synchronization)

- Enhanced throughput (in Load Sharing modes)
- Transparent upgrades

All members in the cluster are aware of the connections passing through each of the other members. The cluster members synchronize their connection and status information across a secure synchronization network.

The glue that binds the members in a ClusterXL cluster is the Cluster Control Protocol (CCP), which is used to pass synchronization and other information between the cluster members.

High Availability

In a High Availability cluster, only one member is active (Active/Standby operation). In the event that the active cluster member becomes unavailable, all connections are re-directed to a designated standby without interruption. In a synchronized cluster, the standby cluster members are updated with the state of the connections of the active cluster member.

In a High Availability cluster, each member is assigned a priority. The highest priority member serves as the Security Gateway in normal circumstances. If this member fails, control is passed to the next highest priority member. If that member fails, control is passed to the next member, and so on.

Upon Security Gateway recovery, you can maintain the current active Security Gateway (Active Up), or to change to the highest priority Security Gateway (Primary Up).

ClusterXL High Availability supports IPv4 and IPv6.

Load Sharing

ClusterXL Load Sharing distributes traffic within a cluster so that the total throughput of multiple members is increased. In Load Sharing configurations, all functioning members in the cluster are active, and handle network traffic (Active/Active operation).

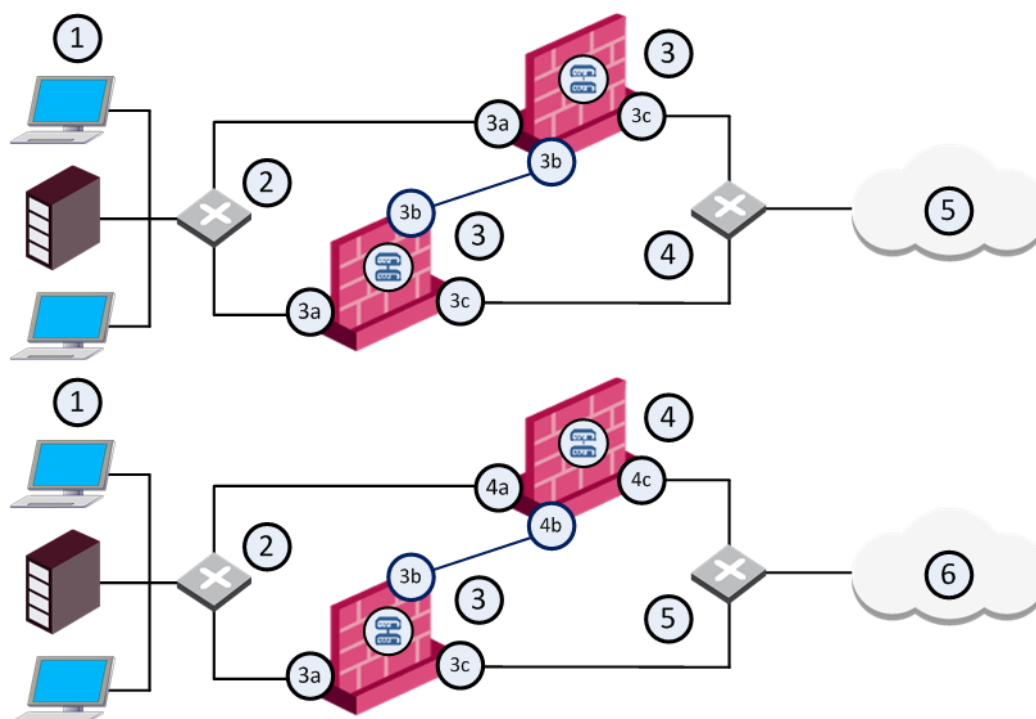
If any member in a cluster becomes unreachable, transparent failover occurs to the remaining operational members in the cluster, thus providing High Availability. All connections are shared between the remaining Security Gateways without interruption.

IPv6 is not supported for Load Sharing clusters.

Example of a ClusterXL Topology

ClusterXL uses unique physical IP and MAC addresses for each **cluster member**, and a virtual IP addresses for the **cluster** itself. Cluster interface addresses do not belong to any real member interface.

The following diagram illustrates a two-member ClusterXL cluster, showing the cluster virtual IP addresses and member physical IP addresses. This sample deployment is used in many of the examples presented in this chapter.



Item	Description
1	Internal network
2	Internal switch (internal cluster IP address 10.10.0.100)
3	Security Gateway - Cluster member A
3a	Virtual interface to the internal network (10.10.0.1)
3b	Interface to the Cluster Sync network (10.0.10.1)
3c	Virtual interface to the external network (192.168.10.1)
4	Security Gateway - Cluster member B
4a	Virtual interface to the internal network (10.10.0.2)
4b	Interface to the Cluster Sync network (10.0.10.2)
4c	Virtual interface to the external network (192.168.10.2)
5	External switch (external routable cluster IP address 192.168.10.100)
6	Internet

Each cluster member has three interfaces: one external interface, one internal interface, and one for synchronization. Cluster member interfaces facing in each direction are connected via a switch, router, or VLAN switch.

All cluster member interfaces facing the same direction must be in the same network. For example, there must not be a router between cluster members.

The Security Management Server can be located anywhere, and should be routable to either the internal or external cluster addresses.

Defining the Cluster Member IP Addresses

The guidelines for configuring each cluster member are as follows:

All members within the cluster must have at least three interfaces:

- An interface facing the external cluster interface, which in turn faces the internet.
- An interface facing the internal cluster interface, which in turn faces the internal network.
- An interface to use for synchronization.

All interfaces pointing in a certain direction must be on the same network.

For example, in the previous illustration, there are two cluster members, Member_A and Member_B. Each has an interface with an IP address facing the Internet through a hub or a switch. This is the external interface with IP address 192.168.10.1 on Member_A and 192.168.10.2 on Member_B, and is the interface that the cluster external interface sees.



Note - This release presents an option to use only two interfaces per member, one external and one internal and to run synchronization over the internal interface. This configuration is not recommended and should be used for backup only.

Defining the Cluster Virtual IP Addresses

In the previous illustration, the IP address of the cluster is **192.168.10.100**.

The cluster has one external virtual IP address and one internal virtual IP address. The external IP address is **192.168.10.100**, and the internal IP address is **10.10.0.100**.

The Synchronization Network

State Synchronization between cluster members ensures that if there is a failover, connections that were handled by the failed member will be maintained. The synchronization network is used to pass connection synchronization and other state information between cluster members. This network therefore carries all the most sensitive security policy information in the organization, and so it is important to make sure the network is secure. It is possible to define more than one synchronization network for backup purposes.

To secure the synchronization interfaces, they should be directly connected by a cross cable, or in a cluster with three or more members, use a dedicated hub or switch.

Members in a Load Sharing cluster must be synchronized because synchronization is used in normal traffic flow. Members in a High Availability cluster do not have to be synchronized, though if they are not, connections may be lost upon failover.

The previous illustration shows a synchronization interface with a unique IP address on each member. **10.0.10.1** on Member_A and **10.0.10.2** on Member_B.

ClusterXL Modes

ClusterXL has these working modes. This section briefly describes each mode and its relative advantages and disadvantages.

- **High Availability Mode**
- **Load Sharing Multicast Mode**
- **Load Sharing Unicast Mode**

High Availability Mode

The High Availability Mode provides basic High Availability capabilities in a cluster environment. This means that the cluster can provide firewall services even when it encounters a problem, which on a stand-alone Security Gateway would have resulted in a complete loss of connectivity. When combined with Check Point State Synchronization, ClusterXL High Availability can maintain connections through failover events, in a user-transparent manner, allowing a flawless connectivity experience. Thus, High Availability provides a backup mechanism, which organizations can use to reduce the risk of unexpected downtime, especially in a mission-critical environment (such as one involving money transactions over the Internet.)

To achieve this purpose, ClusterXL High Availability mode designates one of the cluster members as the active member, while the other members remain in stand-by mode. The cluster virtual IP addresses are associated with the physical network interfaces of the active member (by matching the virtual IP address with the unique MAC address of the appropriate interface). Thus, all traffic directed at the cluster is actually routed (and filtered) by the active member. The role of each cluster member is chosen according to its priority, with the active member being the one with the highest ranking. Member priorities correspond to the order in which they appear in the **Cluster Members** page of the **Cluster Properties** window. The top-most member has the highest priority. You can modify this ranking at any time.

In addition to its role as a firewall, the active member is also responsible for informing the stand-by members of any changes to its connection and state tables, keeping these members up-to-date with the current traffic passing through the cluster.

Whenever the cluster detects a problem in the active member that is severe enough to cause a failover event, it passes the role of the active member to one of the standby members (the member with the currently highest priority). If State Synchronization is applied, any open connections are recognized by the new active member, and are handled according to their last known state. Upon the recovery of a member with a higher priority, the role of the active member may or may not be switched back to that member, depending on the user configuration.

It is important to note that the cluster may encounter problems in standby members as well. In this case, these members are not considered for the role of active members, in the event of a failover.

Load Sharing Modes - Multicast and Unicast

Load Sharing Multicast Mode - This is an efficient way to handle a high load because the load is distributed optimally between all cluster members. Load Sharing Multicast mode associates a multicast MAC with each unicast cluster IP address. This ensures that traffic destined for the cluster is received by all members. The ARP replies sent by a cluster member will therefore indicate that the cluster IP address is reachable via a multicast MAC address.

Load Sharing Unicast Mode - Some routing devices will not accept ARP replies. For some routers, adding a static ARP entry for the cluster IP address on the routing device will solve the issue. Other routers will not accept this type of static ARP entry.

Another consideration is whether your deployment includes routing devices with interfaces operating in promiscuous mode. If on the same network segment there exists two such routers and a ClusterXL Security Gateway in Load Sharing Multicast mode, traffic destined for the cluster that is generated by one of the routers could also be processed by the other router.

For these cases, use Load Sharing Unicast Mode, which does not require the use of multicast for the cluster addresses.

Failover

Failover is a redundancy operation that automatically occurs if a member is not functional. When this happens, another member takes over for the failed member.

In a High Availability configuration, if one member in a synchronized cluster goes down, another member becomes active and "takes over" the connections of the failed member. If you do not use State Synchronization, existing connections are closed when failover occurs, although new connections can be opened.

In a Load Sharing configuration, if one member in a cluster is unavailable, its connections are distributed among the remaining members. All members in a Load Sharing configuration are synchronized, so no connections are interrupted.

To tell each member that the other members are alive and functioning, the ClusterXL Cluster Control Protocol maintains a heartbeat between cluster members. If after a predefined time, no message is received from a member, it is assumed that the cluster member is down and failover occurs. At this point, another member automatically assumes the functionality of the failed member.

It should be noted that a cluster member may still be operational, but if any of the above tests fail, then the faulty member starts the failover because it has determined that it can no longer function as a member.

Note that more than one cluster member may encounter a problem that will result in a failover event. In cases where all cluster members encounter such problems, ClusterXL will try to choose a single member to continue operating. The state of the chosen member will be reported *as Active Attention*. This situation lasts until another member fully recovers. For example, if a cross cable connecting the cluster members malfunctions, both members will detect an interface problem. One of them will change to the *Down* state, and the other to *Active Attention*.

When Does a Failover Occur?

A failover takes place when one of the following occurs on the active cluster member:

- Any critical device (such as **fwd**) fails. A critical device is a process running on a cluster member that enables the member to notify other cluster members that it can no longer function as a member. The device reports to the ClusterXL mechanism regarding its current state or it may fail to report, in which case ClusterXL decides that a failover has occurred and another cluster member takes over.
- An interface or cable fails.
- The member fails or becomes unstable.
- The Security Policy is uninstalled. When the Security Policy is uninstalled the Security Gateway can no longer function as a firewall. If it cannot function as a firewall, it can no longer function as a cluster member and a failover occurs. Normally a policy is not uninstalled by itself but would be initiated by a user. For more on failovers, see sk62570
<http://supportcontent.checkpoint.com/solutions?id=sk62570>.

Configuring ClusterXL

This procedure describes how to configure the Load Sharing Multicast, Load Sharing Unicast, and High Availability New Modes from scratch. Their configuration is identical, apart from the mode selection in SmartDashboard Cluster object or Cluster creation wizard.

Creating Cluster Members



Important - The hardware for all cluster members must be exactly the same, including:

- CPU
- Motherboard
- Memory
- Number and type of interfaces

To create new cluster members for ClusterXL:

1. Install and configure Check Point Security Gateway for all cluster members. Each member must use the identical version and build. For installation and initial configuration procedures, refer to the *R80.10 Installation and Upgrade Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54829>.

During the installation process, enable ClusterXL and State Synchronization:

- For Gaia members, run `cpconfig` from the command line and select **Enable cluster membership for this gateway**.
- For SecurePlatform and Solaris members, select **Enable cluster membership for this gateway**.
- For Windows members, select **This Gateway is part of a cluster**.

If you did not perform this action during installation, you can always do so by using the **cpconfig** utility at a later time. Run the **cpconfig** from the command line, and select the appropriate options to enable cluster capabilities for that member. You may be asked to reboot the member.

2. Define an IP address for each interface on all members. **Do not define IPv6 addresses for synchronization interfaces.**
3. For VPN cluster members, synchronize member clocks accurately to within one second of each other. If these members are constantly up and running it is usually enough to set the time once. More reliable synchronization can be achieved using NTP or some other time synchronization services supplied by the operating system. Cluster member clock synchronization is not applicable for non VPN cluster functionality.
4. Connect the cluster members to each other and to the networks through switches. For the synchronization interfaces, you can use a cross cable or a dedicated switch. Make sure that each network (internal, external, Synchronization, DMZ, and so on) is configured on a separate VLAN, switch or hub.



Note - You can also perform synchronization over a WAN

Configuring Routing for Client Computers

To configure routing for client computers:

1. Configure routing so that communication with internal networks uses the external cluster virtual IP address. For example, configure a static route such that internal network 10.10.0.0 is accessible through 192.168.2.100.
2. Configure routing so that communication with external networks uses the internal cluster IP address. For example, define the internal network IP address 10.10.0.100 as the default Security Gateway for each computer on the internal side of the router.

Choosing the CCP Transport Mode on the Cluster Members

The ClusterXL Control Protocol (CCP) uses multicast by default, because it is more efficient than broadcast. If the connecting switch cannot forward multicast traffic, it is possible, though less efficient, for the switch to use broadcast to forward traffic.

To change the CCP mode between broadcast and multicast, run:

```
cphaconf set_ccp broadcast|multicast
```

Configuring the Cluster Object and Members

The Check Point Appliance or Open Server Wizard is recommended for enterprise grade appliances and open server platforms.

To create a new cluster with the Appliance or Open Server Wizard:

1. In SmartDashboard, right-click Check Point in the **Network Objects** tree.
2. Select **Security Cluster > Check Point Appliance/Open Server**.
3. In the **Check Point Security Gateway Cluster Creation** window, click Wizard Mode.
4. In the **Cluster General Properties** window, enter or select:
 - Cluster Name - Unique name for the cluster
 - Cluster IPv4 and IPv6 address - Virtual Management IP addresses for this cluster.

Important: You must define a corresponding IPv4 address for every IPv6 address. This release does not support pure IPv6 addresses.

 - **Choose the Cluster Solution** - Select **Check Point ClusterXL** and then select **High Availability** or **Load Sharing**.
5. In the **Cluster Member Properties** window, click Add > New Cluster Member to configure each member.
 - a) Enter the physical IPv4 and IPv6 addresses.

Note: Make sure that you do not define IPV6 address for sync interfaces. The wizard does not let you define an interface with an IPv6 address as a sync interface.
 - b) Enter and confirm the SIC trust activation key.
6. In the **Cluster Topology** window, define a network objective (Role) for each network interface and, if necessary, define the virtual cluster IP addresses.

The wizard automatically calculates the subnet for each network and assigns it to the applicable interface on each member. The calculated subnet shows in the upper section of the window.

The available network objectives are:

- **Cluster Interface** - A cluster interface that connects to an internal or external network. Enter the cluster virtual IP addresses for each network (internal or external). These addresses must be located in the calculated subnet.
- **Cluster Sync Interface** - A cluster synchronization interface. You must define one or more synchronization interfaces for redundancy. If you are using more than one synchronization interface, define which interface is the primary, secondary, or tertiary interface. Synchronization redundancy is not supported on Small Business appliances. On these appliances, you can only select **1st sync** and only for the LAN2/SYNC interface. You cannot configure VLANs on the synchronization interface.

- **Monitored Private** - An interface that is not part of the cluster, but ClusterXL monitors the member state and failover occurs if a fault is detected.
- **Non Monitored Private** - ClusterXL does not monitor the member state and there is no failover.

This option is recommended for the management interface.

7. Click **Next** and then **Finish** to complete the wizard.

After you finish the wizard, we recommend that you open the cluster object and do these procedures:

- Define Anti-Spoofing properties for each interface
- Change the topology type (Internal or External) if necessary
- Configure other Software Blades, features and properties as necessary.

VRRP Cluster

Virtual Router Redundancy Protocol (VRRP) provides dynamic failover of IP addresses from one router to another in the event of failure. This increases the availability and reliability of routing paths via gateway selections on an IP network. Each VRRP router has a unique identifier known as the Virtual Router Identifier (VRID) which is associated with at least one Virtual IP Address (VIP). Neighboring network nodes connect to the VIP as a next hop in a route or as a final destination. Gaia supports VRRP as defined in RFC 3768.

On Gaia, VRRP can be used with or without ClusterXL enabled. The most common use case is with ClusterXL enabled. This guide describes one way of configuring VRRP, known as *Monitored Circuit/Simplified VRRP*, with ClusterXL enabled. To learn about all the ways of configuring VRRP, and to use VRRP without ClusterXL enabled, see the *Gaia Administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54824>.

With ClusterXL enabled, VRRP supports a maximum of one VRID with one Virtual IP Address (VIP) on every interface. Only active/backup environments are supported, and you must configure VRRP so that the same node is the VRRP master for all VRIDs. This means that you must configure each VRID to monitor every other VRRP-enabled interface. You must also configure *priority deltas* to allow failover to the backup node when the VRID on any interface does a failover.

Monitored Circuit/Simplified VRRP makes possible a complete node failover by automatically monitoring all VRRP-enabled interfaces. You configure one VRID, and this VRID is automatically added to all the VRRP interfaces. If the VRID on any interface fails, the configured priority delta is decremented on the other interfaces. This allows the backup node to take over as the VRRP master.

How VRRP Failover Works

Each Virtual Router (VRRP Group) is identified by a unique *Virtual Router ID (VRID)*. A Virtual Router contains one *Master Security Gateway*, and at least one *Backup Security Gateway*. The master sends periodic VRRP advertisements (known as *hello messages*) to the backups.

VRRP advertisements broadcast the operational status of the master to the backups. Gaia uses dynamic routing protocols to advertise the VIP (virtual IP address or backup address) of the Virtual Router.

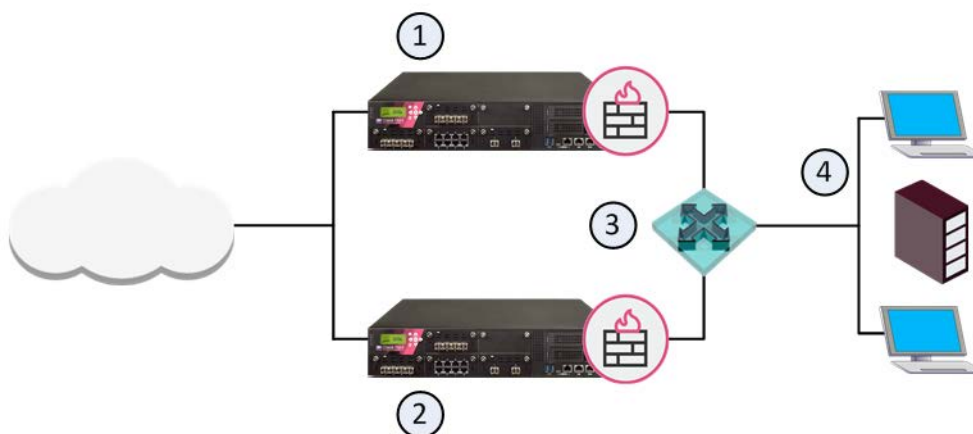
If the master or its interfaces fails, VRRP uses a priority algorithm to decide if failover to a backup is necessary. Initially, the master is the Security Gateway that has the highest defined priority value. You define a priority for each Security Gateway when you create a Virtual Router or change its configuration. If two Security Gateways have same priority value, the platform that comes online and broadcasts its VRRP advertisements first, becomes the master.

Gaia also uses priorities to select a backup Security Gateway upon failover (when there is more than one backup available). In the event of failover, the Virtual Router priority value is decreased by a predefined *Priority Delta* value to calculate an *Effective Priority* value. The Virtual Router with the highest effective priority becomes the new master. The *Priority Delta* value is a Check Point proprietary parameter that you define when configuring a Virtual Router. If you configure your system correctly, the effective priority will be lower than the backup gateway priority in the other Virtual Routers. This causes the problematic master to fail over for the other Virtual Routers as well.

Note- If the effective priority for the current master and backup are the same, the Gateway with the highest IP address becomes the master.

Internal Network High Availability

This is a simple VRRP high availability use case where Security Gateway 1 is the master and Security Gateway 2 is the backup. Virtual Router redundancy is available only for connections to and from the internal network. There is no redundancy for external traffic.



Item	Description
1	Master Security Gateway
2	Backup Security Gateway
3	Virtual Router VRID 5 - Virtual IP Address (Backup Address) is 192.168.2.5
4	Internal Network and hosts

Preparing a VRRP Cluster

Do these steps before you start to define a Virtual Router (VRRP Group).

1. Synchronize the system time on all Security Gateways to be included in this Virtual Router.
Best Practice - We recommend that you enable NTP (Network Time Protocol) on all Security Gateways.
 You can also manually change the time and time zone on each Security Gateway to match the other members. In this case, you must synchronize member times to within a few seconds.
2. Optional: Add host names and IP address pairs to the host table on each Security Gateway.
 This lets you use host names as an alternative to IP addresses or DNS servers.

Configuring Network Switches

Best Practice - If you use the Spanning Tree protocol on Cisco switches connected to Check Point VRRP clusters, we recommend that you enable PortFast. PortFast sets interfaces to the Spanning Tree forwarding state, which prevents them from waiting for the standard forward-time interval.

If you use switches from a different vendor, we recommend that you use the equivalent feature for that vendor. If you use the Spanning Tree protocol without PortFast, or its equivalent, you may see delays during VRRP failover.

Enabling Virtual Routers

When you log into Gaia for the first time after installation, you must use the First Time Wizard to the initial configuration steps. To use VRRP Virtual Routers (clusters), you must first enable VRRP clustering in the First Time Wizard.

To enable VRRP clustering:

1. Install Gaia using the instructions in the *R80.10 Installation and Upgrade Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54829>.
2. On the First Time Wizard **Products** page, select Security Gateway.
Do not select Security Management. The standalone environment (Security Gateway and Security Management Server) is not supported for VRRP.
3. Select **Unit is part of a cluster**.
4. Select **VRRP Cluster** from the list.
5. Continue with the next steps in the wizard.
6. When prompted to reboot the Security Gateway, click **Cancel**.
Do not reboot.
7. Do one of these steps:
 - Run `cpconfig` on the Security Gateway. Select **Enable cluster membership for this gateway** to enable Firewall synchronization.

Note - This is the most common use and does not support active/active mode. You must configure VRRP so that the same cluster member is the VRRP master on all interfaces. Dynamic routing configuration must match on each cluster member.

OR:
 - Do not enable ClusterXL.

Note - This is useful when each cluster member is required to be the VRRP master at the same time. You can configure two VRRP Virtual Routers on the same interface. Each cluster member can be the VRRP master for a different VRID on the same interface while it backs up the other. This configuration can also help run VRRP in a High-Availability pair with a device from another vendor. Disable the VRRP monitoring of the Firewall when you use this configuration. It is enabled by default but not supported with this configuration. Also, only Static Routes are supported with this configuration
8. Enter `y` when prompted.
9. Reboot the Security Gateway.

Do this procedure for each Virtual Router member.

When you complete this procedure for each VRRP member, do these steps in the WebUI:

1. Select **VRRP** from the navigation tree.
2. Make sure that the **Disable All Virtual Routers** option is not selected.

When you complete these procedures, define your Virtual Routers using the WebUI or the CLI.

Configuring Global Settings for VRRP

This section includes shows you how to configure the global settings. Global settings apply to all Virtual Routers.

Configure these global settings:

Cold Start Delay - Delay period in seconds before a Security Gateway joins a Virtual Router.
Default = 0.

Interface Delay - Configure this when the Preempt Mode of VRRP has been turned off. This is useful when the VRRP node with a higher priority is rebooted but must not preempt the existing VRRP master that is handling the traffic but is configured with a lower priority. Sometimes interfaces that come up take longer than the VRRP timeout to process incoming VRRP Hello packets. The *Interface Delay* extends the time that VRRP waits to receive Hello packets from the existing master.

Disable All Virtual Routers - Select this option to disable all Virtual Routers defined on this Gaia system. Clear this option to enable all Virtual Routers. By default, all Virtual Routers are enabled.

Monitor Firewall State - Select this option to let VRRP monitor the Security Gateway and automatically take appropriate action. This is enabled by default, which is the recommended setting when using VRRP with ClusterXL enabled. This must be disabled when using VRRP with ClusterXL disabled.

Important - If you disable **Monitor Firewall State**, VRRP can assign master status to a Security Gateway before it completes the boot process. This can cause more than one Security Gateway in a Virtual Router to have master status.

Configuration Notes

Gaia starts to monitor the firewall after the cold start delay completes. This can cause some problems:

- If all the Security Gateway (member) interfaces in a Virtual Router fail, all Security Gateways become backups. None of the Security Gateways can become the master and no traffic is allowed.
- If you change the time on any of the Security Gateways (member), a failover occurs automatically.
- In certain situations, installing a firewall policy causes a failover. This can happen if it takes a long time to install the policy.

Configuring Monitored Circuit/Simplified VRRP - WebUI

This section includes the basic procedure for configuring a Virtual Router using the Gaia WebUI.

To add a new Virtual Router:

1. In the navigation tree, select **VRRP**.
2. In the **Virtual Routers** section, click **Add**.
3. In the **Add Virtual Router** window, configure these parameters:
 - **Virtual Router ID** - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.
 - **Priority** - Enter the priority value, which selects the Security Gateway that takes over in the event of a failure. The Security Gateway with the highest available priority becomes the new master. The range of valid values 1 to 254. The default setting is 100.
 - **Hello Interval** - (optional) Select the number of seconds, after which the master sends its VRRP advertisements. The valid range is between 1 (default) and 255 seconds.

All VRRP routers on a Security Gateways must be configured with the same hello interval.

Otherwise, more than one Security Gateway can be in the master state.

The hello interval also defines the failover interval (the time a backup router waits to hear from the existing master before it takes on the master role). The value of the failover interval is three times the value of the hello interval (default - 3 seconds).

- **Authentication:**
none - No authentication necessary
simple - A password is required for authentication

You must use the same authentication method for all Security Gateways in a Virtual Router.

If you select **simple**, enter a password in the applicable field.

- **Priority Delta** - Enter the value to subtract from the **Priority** to create an effective priority when an interface fails. The range is 1-254.

If an interface fails on the backup, the value of the priority delta is subtracted from its priority. This gives a higher effective priority to another Security Gateway member.

If the effective priority of the current master is less than that of the backup, the backup becomes the master for this Virtual Router. If the effective priority for the current master and backup are the same, the gateway with the highest IP address becomes the master.

4. In the **Backup Addresses** section, click **Add**. Configure these parameters in the **Add Backup Address** window:

- **IPv4 address** - Enter the interface IPv4 address.
- **VMAC Mode** - Select one of these Virtual MAC modes:
 - **VRRP** - Sets the VMAC to use the standard VRRP protocol. It is automatically set to the same value on all Security Gateways in the Virtual Router. This is the default setting.
 - **Interface** - Sets the VMAC to the local interface MAC address. If you define this mode for the master and the backup, the VMAC is different for each. VRRP IP addresses are related to different VMACs. This is because they are dependent on the physical interface MAC address of the currently defined master.
Note - If you configure different VMACs on the master and backup, you must make sure that you select the correct proxy ARP setting for NAT.
 - **Static** - Manually set the VMAC address. Enter the VMAC address in the applicable field.
 - **Extended** - Gaia dynamically calculates and adds three bytes to the interface MAC address to generate more random address. If you select this mode, Gaia constructs the same MAC address for master and backups in the Virtual Router.
Note - If you set the VMAC mode to Interface or Static, syslog error messages show when you restart the computer or during failover. This is caused by duplicate IP addresses for the master and backup. This is expected behavior because the master and backups temporarily use the same virtual IP address until they get master and backup status.

Click **Save**. The new VMAC mode shows in the in the **Backup Address** table.

5. To remove a backup address, select an address and click **Delete**. The address is removed from the **Backup Address** table.
6. Click **Save**.

Configuring the VRRP Security Gateway Cluster in SmartDashboard

1. From the **Networks Objects** tree, select **Check Point > Security Cluster > Check Point appliance/ Open Server**.

The **Security Gateway Cluster Creation** window opens

2. Choose **Wizard Mode**.
3. Define the:
 - **Cluster Name**
 - **Cluster IPv4 Address**
 - For an IPv6 cluster: **Cluster IPv6 Address**
4. Choose the **Cluster's Solution: Gaia VRRP**.
5. Click **Finish**.

Configuring VRRP Rules for the Security Gateway

1. Define this rule above the Stealth Rule in the Rule Base:

Source	Destination	VPN	Services & Applications	Action
Firewalls (Group) fwcluster-object	mcast-224.0.0.1	Any	vrrp igmp	Accept

Where:

- **Firewalls** -Simple Group object containing the firewall objects.
 - **fwcluster-object** - the VRRP cluster object.
 - **mcast-224.0.0.18** - Node Host object with the IP address 224.0.0.18.
2. If your Security Gateways use dynamic routing protocols (such as OSPF or RIP), create new rules for each multicast destination IP address.

Alternatively, you can create a Network object to show all multicast network IP destinations with these values:

- Name: **MCAST.NET**
- IP: **224.0.0.0**
- Net mask: **240.0.0.0**

You can use one rule for all multicast protocols you agree to accept, as shown in this example:

Source	Destination	VPN	Services & Applications	Action
cluster_all_IPs	fwcluster-object MCAST.NET	Any	vrrp igmp ospf rip	Accept

To Learn More About Maximizing Network Performance

To learn more about maximizing network performance and redundancy, see these R80.10 guides:

- CoreXL, SecureXL and Multi-Queue - *Performance Tuning Administration Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54765>
- ClusterXL - *Cluster XL Administration Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54804>
- VRRP, including Advanced VRRP - *Gaia Administration Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54824>

Simplifying Security for Private Clouds

In This Section:

Introduction to Virtual Systems (VSX).....	175
VSX Architecture and Concepts	178
Configuring a VSX Cluster	184
To Learn More About VSX.....	190

Introduction to Virtual Systems (VSX)

VSX Overview

VSX (Virtual System Extension) is a security and VPN solution for large-scale environments. VSX provides comprehensive protection for multiple networks or VLANs within complex infrastructures. It securely connects them to shared resources such as the Internet and/or a DMZ, and allows them to safely interact with each other.

VSX incorporates the same patented Stateful Inspection and Software Blades technology used in the Check Point Security Gateway product line. Administrators manage VSX using a Security Management Server or a Multi-Domain Server, delivering a unified management architecture for enterprises and service providers. The management server can be installed on a different machine than VSX, or on the same machine.

A VSX Gateway contains a complete set of virtual devices that function as physical network components, such as Security Gateway, routers, switches, interfaces, and even network cables. Centrally managed, and incorporating key network resources internally, VSX lets businesses deploy comprehensive firewall and VPN functionality, while reducing hardware investment and improving efficiency.

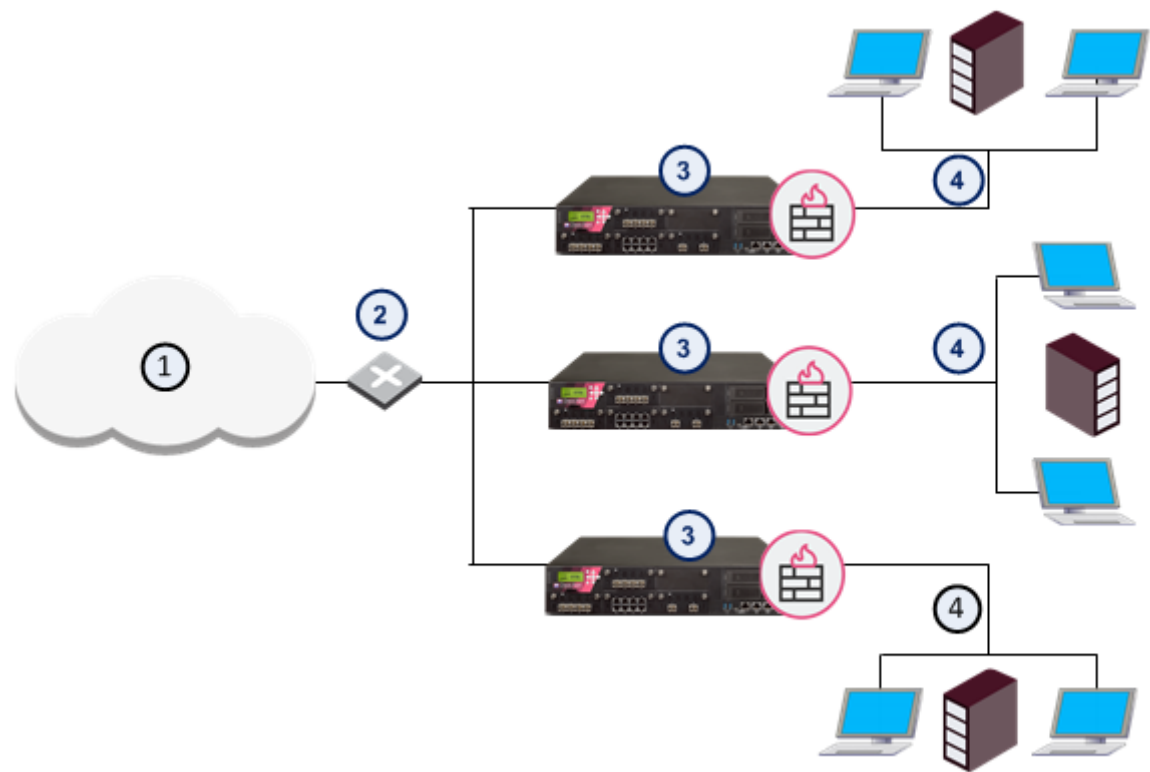
How VSX Works

Each **Virtual System** works as a Security Gateway, typically protecting a specified network. When packets arrive at the VSX Gateway, it sends traffic to the Virtual System protecting the destination network. The Virtual System inspects all traffic and allows or rejects it according to rules defined in the security policy.

In order to better understand how virtual networks work, it is important to compare physical network environments with their virtual (VSX) counterparts. While physical networks consist of many hardware components, VSX virtual networks reside on a single configurable VSX Gateway or cluster that defines and protects multiple independent networks, together with their virtual components.

Physical Network Topology

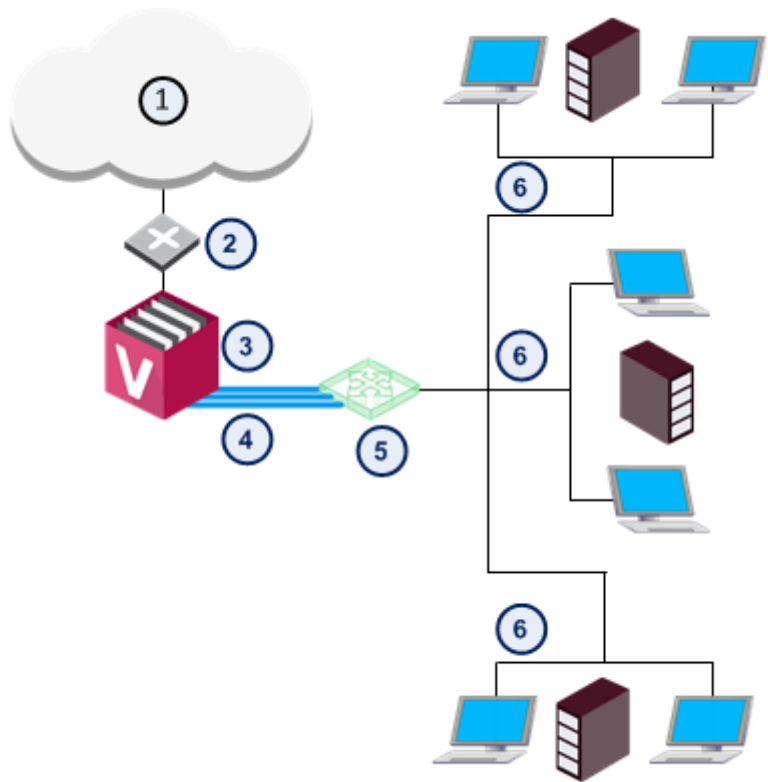
In a typical deployment with multiple Security Gateways, each protects a separate network. Each physical Security Gateway has interfaces to the perimeter router and to the network it protects.



Item	Description
1	Internet
2	Router
3	Security Gateways
4	Network

VSX Virtual Network Topology

Deploy one VSX Gateway with four Virtual Systems to protect multiple networks.



Item	Description
1	Internet
2	Router
3	VSX Gateway. Each Virtual System in a VSX environment is a Security Gateway, with the same security and networking functionality as a physical gateway. Each handles packet traffic to and from the one network it protects.
4	Warp Links. Virtual interfaces and network cables connect the Virtual Systems and the Virtual Switch.
5	Virtual Switch. Connects all the Virtual Systems to the Internet router.
6	Networks

VSX Architecture and Concepts

In This Section:

Virtual Devices	178
Interfaces	179
VSX Clusters.....	181

Virtual Devices

This section describes virtual network components and their characteristics.

Virtual System

A Virtual System is a virtual security and routing domain that provides the functionality of a Security Gateway with full Firewall and VPN facilities. Multiple Virtual Systems can run concurrently on a single VSX Gateway.

Virtual System Autonomy

Each Virtual System functions independently. Each Virtual System maintains its own Software Blades, interfaces, IP addresses, routing table, ARP table, and dynamic routing configuration. Each Virtual System also maintains its own:

- **State Tables:** Each Virtual System has its own kernel tables with configuration and runtime data, such as active connections and IPSec tunnel information.
- **Security and VPN policies:** Each Virtual System enforces its own security and VPN Policies (including INSPECT code). Policies are retrieved from the management server and stored separately on the local disk and in the kernel. In a Multi-Domain Security Management environment, each Domain database is maintained separately on the management server and on the VSX Gateway.
- **Configuration Parameters:** Each Virtual System maintains its own configuration, such as IPS settings and TCP/UDP time-outs. Different Virtual Systems can run in layer-2 or layer-3 mode and co-exist on the same VSX Gateway.
- **Logging Configuration:** Each Virtual System maintains its own logs and runs logging according to its own rules and configuration.

Virtual Routers

A **Virtual Router** is an independent routing domain within a VSX Gateway that performs the functionality of physical routers. Virtual Routers are useful for connecting multiple Virtual Systems to a shared interface, such as the interface leading to the Internet, and for routing traffic from one Virtual System to another. Virtual Routers support dynamic routing.

Virtual Routers perform the following routing functions:

- Packets arriving at the VSX Gateway through a shared interface to the designated Virtual System based on the source or destination IP address.
- Traffic arriving from Virtual Systems directed to a shared interface or to other Virtual Systems.
- Traffic to and from shared network resources such as a DMZ.

Virtual Switches

By providing layer-2 connectivity, a **Virtual Switch** connects Virtual Systems and facilitates sharing a common physical interface without segmenting the existing IP network. As with a physical switch, each Virtual Switch maintains a forwarding table with a list of MAC addresses and their associated ports.

Virtual System in Bridge Mode

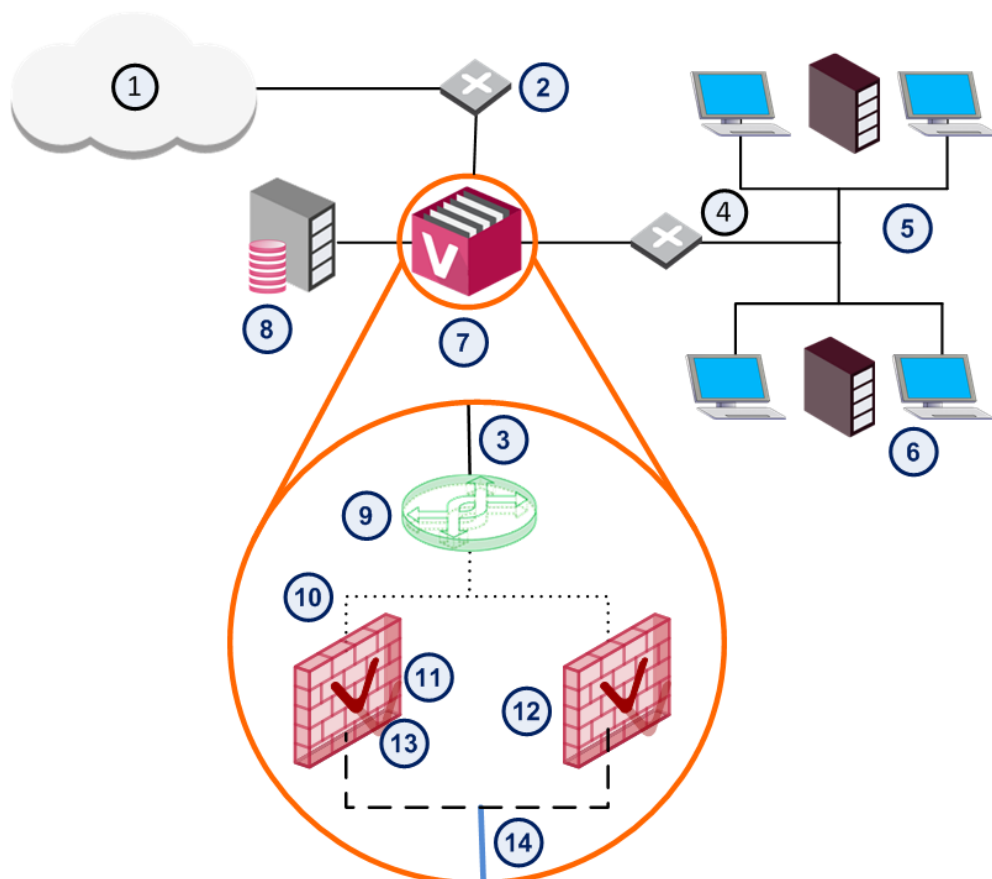
Many Enterprise environments are based on core networks. Situated adjacent to core network backbone switches, VSX protects the internal network by providing security at layer-2, layer-3 or both. VSX communicates with the core network using the existing infrastructure. With Virtual Systems in the Bridge Mode, VSX can protect departmental networks, while simultaneously preventing network segmentation. In this case, switches are located at the entrance to each department's network.

VSX ensures connectivity between the core network and the Internet or external networks, while providing perimeter security. Security can be configured on a per VLAN basis.

Interfaces

The main interface types in VSX are:

- Physical interface
- VLAN interface
- Warp Link



Item	Description
1	Internet
2	Router
3	Physical interface
4	VLAN Switch
5	Network 1
6	Network 2
7	VSX Gateway

Item	Description
8	Security Management Server
9	Virtual Switch
10	Warp Link
11	Virtual System 1
12	Virtual System 2
13	VLAN Interface
14	VLAN Trunk

Notes:

- Warp Links connect the Virtual Switch to each Virtual System.
- A Physical Interface connects the Virtual Switch to an external router leading to the Internet.
- VLAN Interfaces connect the Virtual Systems to the VLAN Switch, via A VLAN trunk.
- The VLAN switch connects to the protected networks.

Physical Interfaces

Physical interfaces connect a VSX Gateway to internal and external networks, as well as to the management server. There are different types of physical interfaces (four types for a VSX Cluster) used in a VSX Gateway:

- **Dedicated Management Interface:** Connects the VSX Gateway to the management server when it is locally managed. If the VSX Gateway is remotely managed, then the management connection arrives via the external or internal interface.
- **External interface:** Connects the VSX Gateway to the Internet or other untrusted networks.
- **Internal Interface:** Connects the VSX Gateway to a protected network.
- **Synchronization Interface:** Connects one VSX Gateway member to other members for state synchronization in a VSX clustering deployment.

VLAN Interfaces

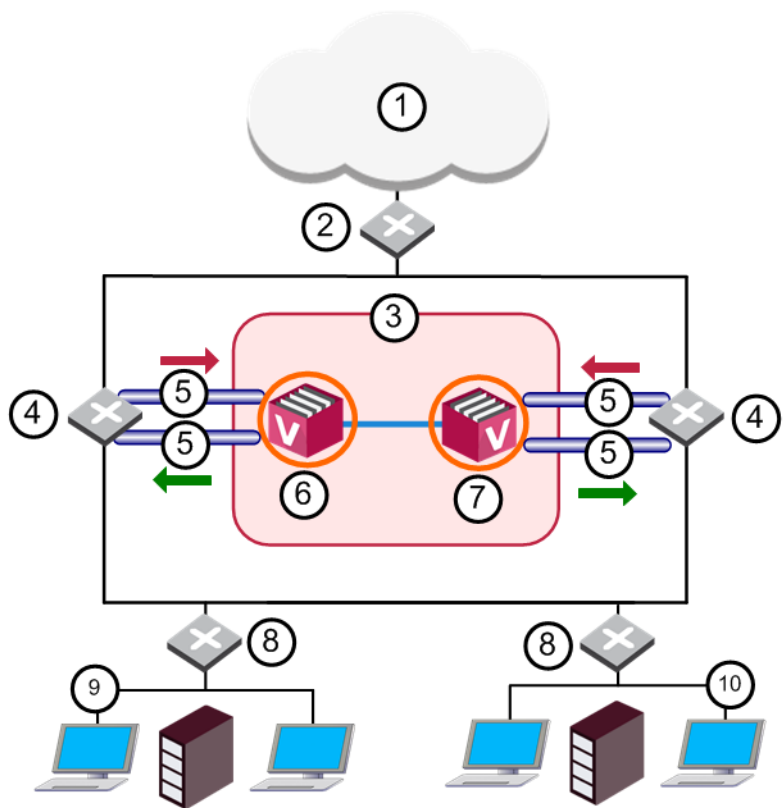
Virtual Systems typically connect to protected VLAN networks using IEEE 802.1q compliant VLAN Interfaces. The networks are connected to ports on an 802.1q-compliant switch that trunks all traffic via a single physical interface to the VSX Gateway.

Warp Links

A Warp Link is a virtual point-to-point connection between a Virtual System and a Virtual Router or Virtual Switch. Each side of a Warp Link represents a virtual interface with the appropriate virtual device.

VSX Clusters

A VSX cluster has two or more identical, interconnected VSX Gateways for continuous data synchronization and transparent failover. Virtual System Load Sharing (VLS) enhances throughput by distributing Virtual Systems, with their traffic load, among multiple, redundant machines.



Item	Description
1	Internet
2	Core Network Backbone switch
3	VSX Cluster
4	Router
5	VLAN
6	Member 1
7	Member 2

Item	Description
8	LAN Switches
9	Sales
10	Finance
	Sync Network
	Physical Interface
	VLAN Trunk

Virtual System Load Sharing (VSLS) Advantages

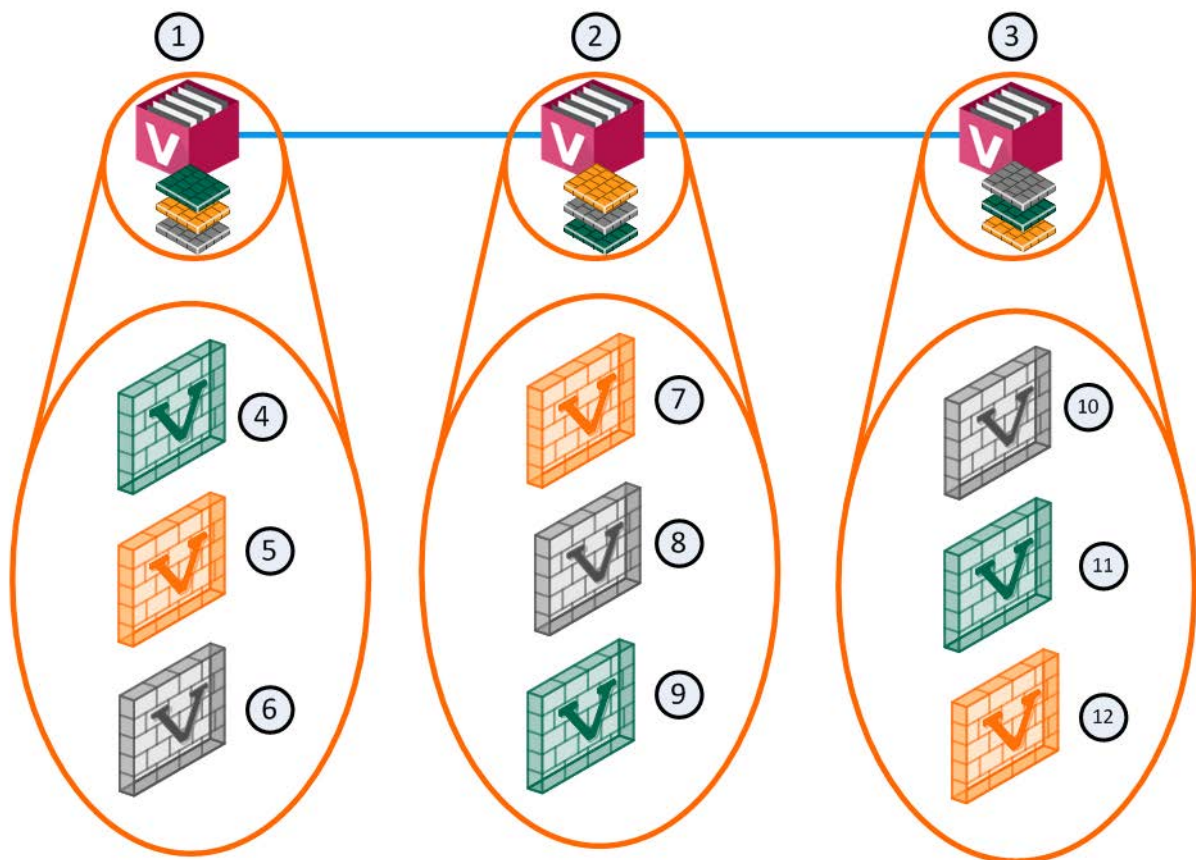
Load Sharing offers significant performance advantages while providing failover for individual Virtual Systems. Using multiple Gateways instead of a single gateway significantly increases performance for CPU intensive applications such as VPNs, Security servers, Policy servers, and Active Directory (LDAP).

By distributing Virtual System instances between different cluster members, the performance load is efficiently spread amongst the members. For example, active Virtual System 1 runs on member A, while active Virtual System 2 runs on member B. Standby and backup Virtual System instances are likewise distributed amongst members to maximize throughput, even in a failover scenario.

VSLS provides an excellent scalability solution, allowing administrators to add additional physical members to an existing VSLS cluster as traffic loads and performance requirements increase.

Virtual System Load Sharing (VSLS) Deployment Scenario

In a deployment scenario with three cluster members, each with three Virtual Systems: an equalized Load Sharing deployment might have one active Virtual System on each cluster member.



Item	Description
1	Member 1
2	Member 2
3	Member 3
4	VS 1 Active
5	VS 2 Standby
6	VS 3 Backup
7	VS 1 Standby

Item	Description
8	VS 2 Backup
9	VS 3 Active
10	VS 1 Backup
11	VS 2 Active
12	VS 3 Standby
	Sync Network

A different member hosts the active peer for each Virtual System. This distribution spreads the load equally amongst the members. When you create a Virtual System, VSX automatically assigns standby and backup states to the appropriate peers and distributes them among the other cluster members.

In the event that a cluster member fails, VSLS directs traffic destined to affected Virtual Systems to their fully synchronized standby peers, which then become active. At the same time, a backup Virtual Systems switches to standby, and synchronizes with the newly active Virtual System.

In the event that an individual active Virtual System fails, it immediately fails over to its standby peer and one of its backup peers becomes the standby, synchronizing with the newly active peer.

Configuring a VSX Cluster

In This Section:

An Example VSX cluster	184
Step 1 - Creating a VSX Cluster	185
Step 2 - Creating a Virtual Switch	188
Step 3 - Creating Virtual System 1	188
Step 4 - Creating Virtual System 2	190
Step 5 - Define the Policy on the Virtual Systems	190

An Example VSX cluster

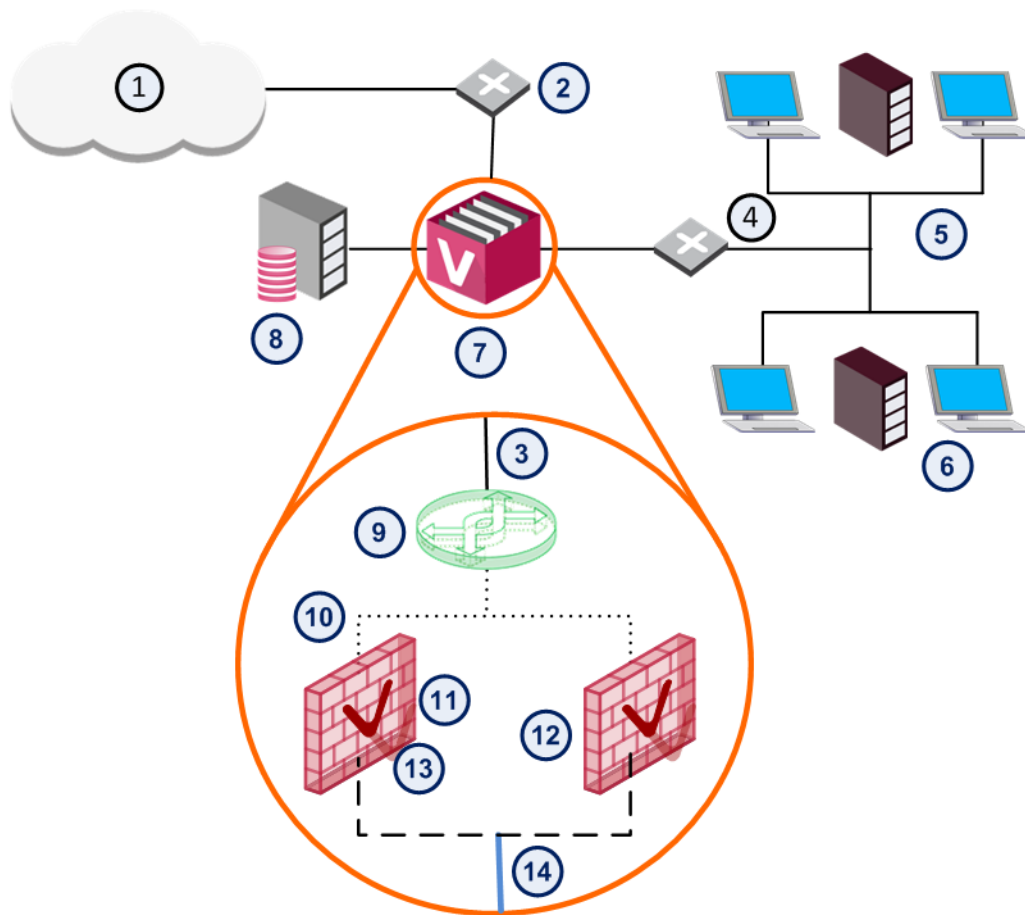
Here we show how to configure a VSX cluster.

Use SmartDashboard for these basic cluster configurations.

In this example, we will:

- Step 1:** Create a VSX cluster with Virtual System Load Sharing (item 7 in the diagram)
- Step 2:** Create virtual switch (item 9)
- Step 3:** Create Virtual System 1 (item 11)
- Step 4:** Create Virtual System 2 (item 12)
- Step 5:** Define the Policy and enable features on the Virtual Systems

You will need the command line interface to add more members, remove members, and upgrade members. Many advanced cluster management procedures require the command line.



Item	Description
1	Internet
2	Router
3	Physical interface
4	VLAN Switch
5	Network 1
6	Network 2
7	VSX Gateway

Item	Description
8	Security Management Server
9	Virtual Switch
10	Warp interface
11	Virtual System 1
12	Virtual System 2
13	VLAN Interface
14	VLAN Trunk

Step 1 - Creating a VSX Cluster

This section describes how to create a new VSX cluster using the **VSX Cluster Wizard**. The wizard guides you through the steps to configure a VSX cluster.

After completing the VSX Cluster Wizard, you can modify most cluster and member properties directly from SmartDashboard.

To create a new cluster:

1. Open SmartConsole.
If you are using Multi-Domain Security Management, open SmartDashboard from the Domain Management Server in which you are creating the cluster.
2. From the click **New** and then select **VSX > Cluster**.
The **VSX Cluster Wizard > General Properties** opens.

Defining Cluster General Properties

The **Cluster General Properties** page contains basic identification properties for VSX clusters.

- **VSX Cluster Name:** Unique, alphanumeric name for the cluster. The name cannot contain spaces or special characters except the underscore.
- **VSX Cluster IP Address:** IP address of the cluster. (In R80, use IPv4.)
- **VSX Cluster Version:** VSX version to use for this cluster.
- **VSX Cluster Platform:** Platform type hosting the cluster members.
 - To create a HA cluster, select **Check Point SecurePlatform (ClusterXL)** from the list
 - To create a Load Sharing (VSLS) cluster, **Check Point ClusterXL Virtual System Load Sharing** select from the list.



Note - All cluster members must use the type of platform, with the same specifications and configuration.

Selecting Creation Templates

Select **Custom Configuration**. You manually create a custom configuration without any template.

Adding Members

The VSX Cluster Members window defines the members of the new cluster. You must define at least two cluster members, and up to as many as eight members. You can add new members later.

To add a new cluster member:

1. In the **VSX Cluster Members** window, click **Add**.
2. The **Member Properties** window opens.
3. Enter the name and IP addresses for the cluster member.
Note: If you define an IPv6 IP address you must also have an IPv4 address.
4. Enter and confirm the activation key to initialize SIC trust between the cluster member and the management server.
5. Follow these steps for all cluster members.
6. Click **Next** to continue.

Defining Cluster Interfaces

The **VSX Cluster Interfaces** window lets you define physical interfaces as VLAN trunks. The list shows all interfaces currently defined on the VSX Gateway or cluster object.

To configure a VLAN trunk:

Select one or more interfaces to define them as VLAN trunks. You can clear an interface to remove the VLAN trunk assignment.



Important - You cannot define the management interface as a VLAN trunk. To use a VLAN as the management interface, you must define the VLAN on the Security Gateway before you use SmartDashboard to create the VSX Gateway.

Configuring Cluster Members

If you selected the custom configuration option, the **VSX Cluster Members** window appears. In this window, you define the synchronization IP address for each member.

To configure the cluster members:

1. Select the synchronization interface from the list.
2. Enter the synchronization interface addresses and net mask for each member.

Cluster Management

The **VSX Gateway Management** page allows you to define several security policy rules that protect the cluster itself. This policy is installed automatically on the new VSX cluster.



Note - This policy applies **only** to traffic destined for the cluster. Traffic destined for Virtual Systems, other virtual devices, external networks, and internal networks is not affected by this policy.

The security policy consists of predefined rules covering the following services:

- **UDP**: SNMP requests
- **TCP**: SSH traffic
- **ICMP**: Echo-request (ping)
- **TCP**: HTTPS (secure HTTP) traffic

Configuring the Cluster Security Policy

1. **Allow**: Enable a rule to allow traffic for those services for which you wish to allow traffic. Clear a rule to block traffic. By default, all services are blocked.

For example, you may wish to allow UDP echo-request traffic in order to be able to ping cluster members from the management server.

2. **Source**: Click the arrow and select a **Source Object** from the list. The default value is ***Any**. Click **New Source Object** to define a new source.

Completing the Wizard

To complete the VSX Cluster Wizard:

1. Click **Next** to continue and then click **Finish** to complete the VSX Cluster wizard.
It can take several minutes to complete. A message appears indicating successful or unsuccessful completion of the process.
If the process ends unsuccessfully, click **View Report** to view the error messages. Refer to the troubleshooting steps for more information.
2. In SmartConsole, double-click the new VSX Cluster object.

Step 2 - Creating a Virtual Switch

Use the **Virtual Switch Wizard** to create a new Virtual Switch. You can modify the initial definition and configure advanced options after completing the wizard.

To create a new Virtual Switch:

1. Open SmartConsole.
2. From the **Objects Bar (F11)**, click **New > More > Network Object > Gateways and Servers > VSX > Virtual Switch**.

The **General Properties** page of the **Virtual Switch Wizard** opens.

3. Enter the name of the Virtual Switch.
4. Select the VSX Gateway or cluster to which the Virtual Switch connects.
5. Click **Next**.
6. Click **Add**.

The **Add Interface** window opens.

7. In the **Add Interface** window, configure the interface on the Virtual Switch.
8. Click **OK** and then click **Next**.
9. Click **Finish**.

Step 3 - Creating Virtual System 1

You use the **Virtual Systems Wizard** to create a new Virtual System.

In this example configuration ("[Configuring a VSX Cluster](#)" on page 184), create Virtual System 1.

You can modify the initial definition and configure advanced options after you complete the wizard.

To start the Virtual System **wizard**:

1. Open SmartDashboard.
2. Right-click the VSX Gateway and select **VSX > Virtual System**.

The **Virtual System Wizard** opens.

Defining General Properties

The **General Properties** wizard page defines the Virtual System object and the hosting VSX Gateway.

These are the parameters in this page:

- **Name:** Unique, alphanumeric for the Virtual System. The name cannot contain spaces or special characters except the underscore.
- **VSX Cluster / Gateway:** Select the VSX Gateway that is hosting the Virtual System.
- **Bridge Mode:** Select this option to create a Virtual System in the Bridge Mode.
- **Override Creation Template:** Select this option to override the creation template that was used for the initial configuration of the VSX Gateway.

Defining Network Configuration

The Virtual System Network Configuration page allows you to define internal and external interfaces as well as the IP address topology located behind the internal interface.

To configure the external and internal interfaces:

1. In the **Interface** table, define the external and internal interfaces, and links to devices.

You can add new interfaces and delete and change existing interfaces.

To add an interface, click **Add**. The **Interface Properties** window opens. Select an interface from the list and define its properties. Click **Help** for details regarding the various properties and options.

For this example, add two interfaces for each Virtual System:

- One external interface that leads to the Virtual System.
- One internal interface that leads to an available interface with a VLAN tag.

2. Select the **Main IP Address** from the list.

This IP address is usually assigned to the external interface and specifies the Virtual System address used with NAT or VPN connections.

To make an external IP address routable, select the external interface IP address as the main IP address.

3. Define network routing for your deployment.

Some routes are automatically defined by the interface definitions. For example, you define a default gateway route leading to an external Virtual Router or to the Virtual System external interface.

To manually add a default route to the **Routes** table, click **Add Default Routes**. Enter the default route IP address, or select the default Virtual Router. The **Route Configuration** window opens.

4. Complete the definition ("[Completing the Definition](#)" on page 190).

Completing the Definition

Click **Next** and then **Finish** to create the Virtual System. Please note that this may take several minutes to complete. A message appears indicating successful or unsuccessful completion of the process.

If the process ends unsuccessfully, click **View Report** to view the error messages.

After you create a Virtual System using the Virtual System Wizard, you can modify the topology and all other parameters (except the name of the Virtual System) using the **Virtual System Properties** window.

Step 4 - Creating Virtual System 2

Use the **Virtual Systems Wizard** to create a new Virtual System.

In this example configuration ("[Configuring a VSX Cluster](#)" on page 184), create Virtual System 2.

Follow the instructions in Step 3 - Creating Virtual Systems 1 ("[Step 3 - Creating Virtual System 1](#)" on page 188).

Step 5 - Define the Policy on the Virtual Systems

Define the Policy and enable features on the Virtual Systems. The procedures for this are the same as on a Security Gateway.

For more about Security Policies, see the *R80.10 Security Management Administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54842>.

To Learn More About VSX

To learn more about simplifying security for private clouds using VSX, see the *R80.10 VSX Administration Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54764>.

Securing Data

In This Section:

Overview	191
Enabling DLP	192
DLP Rule Base	194
Analyzing and Tracking DLP	197
To Learn More About Data Loss Prevention	198

Overview

Data is more accessible and transferable today than ever before, and the vast majority of data is sensitive at different levels. Some is confidential simply because it is part of an internal organization and is not meant to be available to the public. Some data is sensitive because of corporate requirements and legal regulations.

The Check Point Data Loss Prevention Software Blade (DLP) lets you use the Firewall to prevent users from sending sensitive data to external networks. DLP helps you implement an automated corporate policy that catches sensitive and protected data before it leaves your organization.

Data Loss Prevention Features

These are the features that the Data Loss Prevention Software Blade uses:

- **UserCheck™** - Lets users handle data loss incidents with automated user notification and the unique **Ask User** mode. Each person in your organization learns the best practices to prevent future accidental leaks. These are the majority of DLP incidents and they can be handled quickly with the DLP Self Incident Handling Portal or the UserCheck client ("**UserCheck Actions**" on page 44).
- **MultiSpect™** - Unmatched accuracy to identify and prevent incidents. DLP uses multi-parameter correlation with different customizable data types and with CPcode.
- **Out of the Box Security** - A rich set of defined data types recognizes sensitive forms, templates and data. DLP has a good out-of-the-box policy to make sure that the data stays in the internal network.
- **Data Owner Auditing** - Data Owners are the users in the organization that control the information and files for their own area or department. They get timely automated notifications and reports that show how their data is being moved. Without Data Owner control, system administrators can frequently be placed in an awkward position between managers and employees.
- **CPcode™** - DLP supports fully customized data identification through the use of CPcode. You can define how email data matches DLP policies and rules.



Note - See the *R77 CPcode DLP Reference Guide*

http://supportcontent.checkpoint.com/documentation_download?ID=24804.

Using a Mail Relay and Mail Server

You can configure the Security Gateway to send email notifications to users and Data Owners. If you are using email notifications, it is necessary for the Security Gateway to access a mail server and a mail relay.

We recommend that you use different computers for a mail server and a mail relay. For more about other deployments, see the *R80.10 DLP Administration Guide*

<http://downloads.checkpoint.com/dc/download.htm?ID=54805>.

Enabling DLP

You can configure a DLP rule that sends users to the DLP portal when they send questionable data. This rule lets users decide if they will send data that can potentially violate the security policy.

The DLP portal is a web page that informs users that the specified data is possibly against company policy. If the users **Send** the data, then the action is logged.



Important - If you are using Data Owners, it is necessary to configure a mail server in the **DLP Portal and Mail Server** window.

To enable DLP on an existing Security Gateway or cluster:

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 the **General Properties** view.
3. In the **Network Security** tab, select **Data Loss Prevention**.
The **Data Loss Prevention Wizard** opens.
4. Click **Next**.
The **Email Domain and Active Directory** page opens.
5. Enter the email domain for your company to let DLP distinguish between internal and external email addresses.
6. **Optional:** To enable the Security Gateway to access user information in an AD, enter the AD user name and password.
The Security Gateway accesses information in the definition of **My Organization**.
7. Click **Next**.
The **My Organization Name** page opens.
8. Enter different names and phrases that are used to identify your organization.
DLP uses these names to accurately detect incidents of data loss.
9. Click **Next**.
The **DLP Portal and Mail Server** page opens.
10. **Optional:** Enable the DLP portal.
NOTE: It is not necessary to enable the DLP portal if UserCheck is enabled.
 - a) Select **Activate DLP Portal for Self Incident Handling**.
 - b) In **Main URL**, enter the URL for the DLP portal.
11. **Optional:** Enable a mail server to send DLP emails to users about possible DLP incidents.

- a) Select **Mail Server**.
- b) From **Send emails using this mail server**, select a mail server or click **New**.
- c) To create a new mail server, in the **Mail Server** window enter the settings for the mail server and click **OK**.

12. Click **Next**.

The **Protocols** page opens.

13. Select one or more of these protocols to which the DLP policy applies.

- **Email**
- **Web**
- **File Transfer**

14. Click **Next**.

The **Data Loss Prevention Blade Setup is Completed** window opens.

15. Click **Finish**.

Adding Data Owners

When DLP incidents are logged, the DLP gateway can send automatic notifications to the Data Owners.

To add Data Owners to a Data Type:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
SmartDashboard opens and shows the **My Organization** page in the **Data Loss Prevention** tab.
3. From the navigation tree, select **Data Types**.
4. Double-click a data type.
The data type properties window opens.
5. From the navigation tree, select **Data Owners**.
6. Click **Add**.
The **Add Data Owners** window opens.
7. Select the user or group who is responsible for this data and click **Add**.
If the data owner is not in the list, click **New**. In the **Email Addresses** window, enter the name and email address of the data owner (or name a list of email addresses).
8. Add as many data owners as needed.
9. Click **OK**.

Notifying Data Owners

DLP can send automatic messages to Data Owners for incidents that involve the applicable data types.

To configure Data Owner notification:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
SmartDashboard opens and shows the **My Organization** page in the **Data Loss Prevention** tab.
3. From the navigation tree, select **Policy**.

4. Right-click the **Track** cell of the rule and select **Email**.
The **Email** window opens.
5. Select **When data is matched**.
Data Owners are added to the Email Notification list.
6. **Optional:** Click **Add** and add more users to send notification emails to.
7. Use the default notification email message, or click **Customize** and enter the message.
The default message is: The Check Point Data Loss Prevention system has found traffic which matches a rule
8. Click **OK**.

Using DLP with Microsoft Exchange

Internal emails between Microsoft Exchange clients use a proprietary protocol which is not supported by the Security Gateways. To scan internal emails between Microsoft Exchange clients, you must install an Exchange Security Agent on the Exchange Server. The agent sends emails to the Security Gateway for inspection using the SMTP protocol encrypted with TLS. To supply Data Loss Prevention for Microsoft exchange, it is necessary that the Exchange server can communicate with the Security Gateway.

An Exchange Security Agent must be installed on each Exchange Server that sends traffic to the Security Gateway with DLP. Each agent is centrally managed through SmartDashboard and can only send emails to one Security Gateway. If your organization uses Exchange servers for all of its emails, you can also use this setup for scanning all emails.

To use the Exchange Security Agent it is necessary to configure settings in SmartConsole and on the Exchange server. For more about configuring an Exchange Security Agent, see sk103166 <http://supportcontent.checkpoint.com/solutions?id=sk103166>.

DLP Rule Base

The rules in the DLP Rule Base are not applied sequentially, all the rules are applied to each data transmission. If the data matches multiple rules, the most restrictive rule is applied. The order from most restrictive to least is:

1. Rule with an exception
2. Action - Prevent
3. Action - Ask User
4. Action - Inform User
5. Action - Detect

Managing the DLP Rule Base

Use SmartDashboard to create and configure DLP rules.

To open the DLP Rule Base:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
SmartDashboard opens and shows the **My Organization** page in the **Data Loss Prevention** tab.
3. From the navigation tree, click **Policy**.

These are the fields that manage the rules for the DLP Rule Base.

Field	Description
Flag	Mark a rule to Follow Up or Improve Accuracy .
Name	Name of the rule.
Data	Data type for this rule.
Source	Who or what starts the connection: Users and Administrators, network, or email domains. If Identity Awareness is enabled, you can use Access Roles.
Destination	Who or what completes the connection: Users and Administrators, network, or email domains. If Identity Awareness is enabled, you can use Access Roles.
Protocol	Type of network protocol for this rule.
Exceptions	Number of exceptions that allow traffic for this rule.
Action	DLP action that is done when traffic matches the rule.
Track	Tracking and logging action that is done when traffic matches the rule.
Severity	Set the severity level for this rule. Use Severity to help filter Data Loss Prevention incidents with SmartEvent.
Install On	Network objects that will get the rule of the security policy. The Policy Targets option installs the rule on all firewall gateways.
Time	Time period that DLP enforces this rule.
Category	DLP category for this rule.

DLP Rule Exceptions

When a data transmission matches criteria of an exception to a DLP rule, the rule **Action** is not applied. If the data matches two DLP rules, and only one of the rules has an exception, the rule without exceptions is applied.

To create an exception for a DLP rule:

1. In SmartConsole, go to **Manage & Settings > Blades**.
2. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
SmartDashboard opens and shows the **My Organization** page in the **Data Loss Prevention** tab.
3. From the navigation tree, select **Policy**.
The **Policy** window opens and shows the DLP Rule Base.
4. Right-click the **Exceptions** cell for a rule and select **Edit**.
The **Exceptions for Rule** window opens.
5. Click **New Exception**.
6. Configure these settings for the exception: **Data Type**, **Source**, **Destination**, **Protocol**.
7. Click **OK**.
8. Install the policy.

DLP Rule Actions

For each DLP rule that you create for a data type, you also define what action is to be taken if the rule matches a transmission.

Action	Description
Detect	The Firewall sends the data. The event is logged in the Logs & Monitor > Logs view and is available for your review and analysis in the Logs & Monitor Access Control views and SmartEvent. The data and the email itself, or the properties of the transmission if not email, are saved in storage for future reference.
Inform User	The Firewall sends the data, but the incident is logged and the user is notified.
Ask User	The Firewall blocks the data and DLP holds it until the user verifies that it should be sent. A notification, usually with a remediation link to the Self Incident Handling portal, is sent to the user. The user decides whether the transmission should be completed or not. The decision itself is logged in the Logs & Monitor Logs tab of SmartConsole. Look at the predefined query: DLP > User Actions .
Prevent	The Firewall blocks the data. Note: Check Point does not recommend using the Prevent action as a first choice. The action may prove disruptive. To improve the accuracy of rule matches, set rules to Prevent only when you have tested them with the less strict actions over a reasonable amount of time.
Watermark	Tracks Microsoft Office documents (Word, Excel, or PowerPoint files from Office 2007 and higher) and adds visible watermarks or invisible encrypted text. • By default, all rules are created without a watermark action. • Watermarks can be created and edited without having to apply them. • Once a watermark object is created, it can be reused in multiple rules.

Sample Rule Base

This table shows a sample DLP Rule Base. These are the settings for the columns that are not shown:

- **Source** - My Organization
- **Destination** - Outside My Organization
- **Install On** - DLP Blades
- **Protocol** - Any
- **Time** - Any

Flag	Name	Data	Exceptions	Action	Track	Severity	Category
Follow Up	Salesforce Reports	Salesforce Reports	None	Ask User Restricted	Log	High	Business
No Flag	PCI - Credit Card Numbers	PCI - Cardholder Data PCI - Credit Card Numbers	None	Prevent	Log	Critical	Compliance
No Flag	SEC Filings - Draft or Recent	SEC Filings - Draft or Recent	None	Detect	Log Email	High	Financial
No Flag	Source Code	Source Code	1	Detect	Alert	High	Intellectual Property

Salesforce Reports - When users send data that matches the **Salesforce Reports** Data Type category, they are asked to confirm the data transmission. A watermark with the word **Restricted** is added to Microsoft Word, Excel and PowerPoint files. This incident is logged with **High** severity.

PCI - Credit Card Numbers - Users are blocked from sending data that matches the **PCI - Cardholder Data**, and **PCI - Credit Card Numbers** Data Type categories. These incidents are logged with **Critical** severity.

SEC Filings - Draft or Recent - Data transmissions that matches the **SEC Filings - Draft or Recent** Data Type category are logged with **High** severity. An email is sent to the Data Owners for each incident.

Source Code - Data transmissions that matches the **Source Code** Data Type category are logged with **High** severity. A pop-up window opens in SmartView Monitor for each incident.

Analyzing and Tracking DLP

To keep a strong Data Loss Prevention policy, it is necessary to do an analysis of DLP incidents. These clients can help with your DLP analysis:

- The **Logs & Monitor > Logs** tab of SmartConsole
- SmartEvent

You can use the **Follow Up** flag in SmartDashboard for the DLP rules. If you find one or more incidents that you want to change or fine-tune, set the Data Type or rule to **Follow Up**.



Note - To use a Windows 7 computer to view DLP incidents in the **Logs & Monitor > Logs** tab of SmartConsole, or SmartEvent, you must install Microsoft Office 2010. These SmartConsole clients do not show DLP incidents, if these EML files are associated with another application.

Analyzing DLP Incidents in the Logs

You can open the log of an incident and see the actual data that caused the incident. It is not necessary to review most of the incidents manually, but the data transmission (for example, the email or attachment) is saved.



Important - The DLP logs can contain personal emails and web posts that were captured. **You must let the users know** that this can happen. Failure to do so may cause your organization to be in conflict with local privacy laws.

To analyze DLP logs:

1. In SmartConsole, go to **Logs & Monitor**.
2. In **Logs** tab, click **Favorites** (star icon), and select **DLP > Incidents**.
3. Select a time frame in the search field, to refine the list of incidents:
 - **Last Hour**
 - **Today**
 - **Last 24 Hours**
 - **Yesterday**
 - **This Week**
 - **Last 7 Days**
 - **This Month**
 - **Last 30 Days**
 - **All Time**
 - **Custom** - specify the **Start** and **End** date and time in the window that opens, and click **OK**

The Data Loss Prevention logs for the category are shown.

Event Analysis Views Available in SmartConsole

As of R80, the Event Analysis views of the SmartEvent GUI have been incorporated into the SmartConsole Logs & Monitor view. They provide advanced analysis tools with filtering, charts, and statistics of all events that pass through enabled Security Gateways.

To Learn More About Data Loss Prevention

To learn more about securing data, see these guides:

- *R80.10 Data Loss Prevention Administration Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54805>.
- *R77 CPCode Administration Guide*
http://supportcontent.checkpoint.com/documentation_download?ID=24804.