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 R77
For more about this release, see the R77 home page http://supportcontent.checkpoint.com/solutions?id=sk104859.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=24832.
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 Firewall R77 Versions Administration Guide.

Searching in Multiple PDFs
To search for text in all R77 PDF documents, download and extract the complete R77 documentation package http://supportcontent.checkpoint.com/documentation_download?ID=26770. Use Shift-Control-F in Adobe Reader or Foxit reader.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>06 December 2015</td>
<td>Clarified R77.30 Add-on requirement for LTE.</td>
</tr>
<tr>
<td>21 July 2015</td>
<td>Licenses [on page 16] moved to first chapter</td>
</tr>
<tr>
<td>23 June 2015</td>
<td>Correct parameters in Deactivating Session Hijacking Protection [on page 136] Updated instructions for permanently Enabling Syslog in Kernel [on page 142]</td>
</tr>
<tr>
<td>5 May 2015</td>
<td>Added LTE [on page 129]. New for R77.30</td>
</tr>
<tr>
<td>30 November 2014</td>
<td>Added Bidirectional NAT</td>
</tr>
<tr>
<td>9 June 2014</td>
<td>Updated cover with R77 Versions. Applies to R77 and R77.x.</td>
</tr>
<tr>
<td>14 January 2014</td>
<td>Removed documentation for IPS-1 sensor support (discontinued)</td>
</tr>
<tr>
<td>26 August 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Terms</td>
<td>11</td>
</tr>
<tr>
<td>Check Point Firewall Security Solution</td>
<td>14</td>
</tr>
<tr>
<td>Overview of Firewall Features</td>
<td>14</td>
</tr>
<tr>
<td>Components of the Check Point Solution</td>
<td>14</td>
</tr>
<tr>
<td>Dual Stack (IPv4 and IPv6) Network Configuration</td>
<td>15</td>
</tr>
<tr>
<td>Access Control and the Rule Base</td>
<td>16</td>
</tr>
<tr>
<td>Licenses</td>
<td>16</td>
</tr>
<tr>
<td>How to Use this Guide</td>
<td>16</td>
</tr>
<tr>
<td>SmartDashboard Toolbar</td>
<td>18</td>
</tr>
<tr>
<td>Creating a Strong Firewall Security Policy</td>
<td>19</td>
</tr>
<tr>
<td>Using the Firewall Rule Base</td>
<td>19</td>
</tr>
<tr>
<td>Managing the Firewall Rule Base</td>
<td>19</td>
</tr>
<tr>
<td>Explicit and Implied Rules</td>
<td>20</td>
</tr>
<tr>
<td>Order of Rule Enforcement</td>
<td>21</td>
</tr>
<tr>
<td>Creating a Secure Firewall Rule Base</td>
<td>21</td>
</tr>
<tr>
<td>Basic Rules</td>
<td>21</td>
</tr>
<tr>
<td>Sample Firewall Rule Base</td>
<td>22</td>
</tr>
<tr>
<td>Defining Security Zones</td>
<td>22</td>
</tr>
<tr>
<td>Perimeter</td>
<td>23</td>
</tr>
<tr>
<td>DMZ</td>
<td>23</td>
</tr>
<tr>
<td>Preventing IP Spoofing</td>
<td>23</td>
</tr>
<tr>
<td>Configuring Anti-Spoofing</td>
<td>24</td>
</tr>
<tr>
<td>Excluding Specific Internal Addresses</td>
<td>26</td>
</tr>
<tr>
<td>Analyzing the Rule Base (Hit Count)</td>
<td>26</td>
</tr>
<tr>
<td>Enabling or Disabling Hit Count</td>
<td>27</td>
</tr>
<tr>
<td>Configuring the Hit Count Display</td>
<td>27</td>
</tr>
<tr>
<td>Remote Access to the Network</td>
<td>29</td>
</tr>
<tr>
<td>Overview</td>
<td>29</td>
</tr>
<tr>
<td>Check Point Mobile Access Solutions</td>
<td>29</td>
</tr>
<tr>
<td>Client-Based vs. Clientless</td>
<td>30</td>
</tr>
<tr>
<td>Mobile Access Clients</td>
<td>30</td>
</tr>
<tr>
<td>Mobile Access Web Portal</td>
<td>30</td>
</tr>
<tr>
<td>SSL Network Extender</td>
<td>30</td>
</tr>
<tr>
<td>Configuring Remote Access to Network Resources</td>
<td>30</td>
</tr>
<tr>
<td>Sample Mobile Access Workflow</td>
<td>30</td>
</tr>
<tr>
<td>Sample Mobile Access Deployment</td>
<td>31</td>
</tr>
<tr>
<td>Using the Mobile Access Configuration Wizard</td>
<td>32</td>
</tr>
<tr>
<td>Allowing Mobile Connections</td>
<td>33</td>
</tr>
<tr>
<td>Defining Access to Applications</td>
<td>34</td>
</tr>
<tr>
<td>Activating Single Sign On</td>
<td>34</td>
</tr>
<tr>
<td>Connecting to a Citrix Server</td>
<td>35</td>
</tr>
<tr>
<td>Citrix Services</td>
<td>35</td>
</tr>
<tr>
<td>Sample Deployment with Citrix Server</td>
<td>36</td>
</tr>
<tr>
<td>Configuring Citrix Services for Mobile Access</td>
<td>37</td>
</tr>
<tr>
<td>Compliance Check</td>
<td>37</td>
</tr>
<tr>
<td>Compliance Policy Rules</td>
<td>38</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring the NAT Policy</td>
<td>102</td>
</tr>
<tr>
<td>Maximizing Network Performance</td>
<td>98</td>
</tr>
<tr>
<td>Securing Data</td>
<td>86</td>
</tr>
<tr>
<td>Threat Prevention Policies</td>
<td>80</td>
</tr>
<tr>
<td>Anti-Bot and Anti-Virus</td>
<td>80</td>
</tr>
<tr>
<td>Protecting Networks from Bots</td>
<td>80</td>
</tr>
<tr>
<td>Protecting Networks from Viruses</td>
<td>81</td>
</tr>
<tr>
<td>ThreatSpect engine and ThreatCloud repository</td>
<td>81</td>
</tr>
<tr>
<td>Learning about Malware</td>
<td>81</td>
</tr>
<tr>
<td>Examining Anti-Bot and Anti-Virus Protections</td>
<td>82</td>
</tr>
<tr>
<td>Enabling the Anti-Bot Software Blade</td>
<td>82</td>
</tr>
<tr>
<td>Anti-Bot and Anti-Virus Rule Base</td>
<td>82</td>
</tr>
<tr>
<td>Sample Rule Base</td>
<td>84</td>
</tr>
<tr>
<td>Anti-Spam</td>
<td>84</td>
</tr>
<tr>
<td>Enabling Anti-Spam</td>
<td>84</td>
</tr>
<tr>
<td>Sample Configuration</td>
<td>85</td>
</tr>
<tr>
<td>Securing Data</td>
<td>86</td>
</tr>
<tr>
<td>Overview</td>
<td>86</td>
</tr>
<tr>
<td>Data Loss Prevention Features</td>
<td>86</td>
</tr>
<tr>
<td>Sample DLP Deployment</td>
<td>87</td>
</tr>
<tr>
<td>Using a Mail Relay and Mail Server</td>
<td>88</td>
</tr>
<tr>
<td>Enabling DLP</td>
<td>89</td>
</tr>
<tr>
<td>Adding Data Owners</td>
<td>90</td>
</tr>
<tr>
<td>Notifying Data Owners</td>
<td>90</td>
</tr>
<tr>
<td>Using DLP with Microsoft Exchange</td>
<td>91</td>
</tr>
<tr>
<td>DLP Rule Base</td>
<td>91</td>
</tr>
<tr>
<td>Managing the DLP Rule Base</td>
<td>91</td>
</tr>
<tr>
<td>DLP Rule Exceptions</td>
<td>92</td>
</tr>
<tr>
<td>DLP Rule Actions</td>
<td>92</td>
</tr>
<tr>
<td>Sample Rule Base</td>
<td>93</td>
</tr>
<tr>
<td>Analyzing and Tracking DLP</td>
<td>94</td>
</tr>
<tr>
<td>Using SmartView Tracker</td>
<td>94</td>
</tr>
<tr>
<td>Using SmartEvent</td>
<td>97</td>
</tr>
<tr>
<td>Maximizing Network Performance</td>
<td>98</td>
</tr>
<tr>
<td>Check Point Software Acceleration Solutions</td>
<td>98</td>
</tr>
<tr>
<td>CoreXL</td>
<td>98</td>
</tr>
<tr>
<td>Configuring CoreXL</td>
<td>99</td>
</tr>
<tr>
<td>Using SecureXL</td>
<td>99</td>
</tr>
<tr>
<td>Configuring SecureXL</td>
<td>100</td>
</tr>
<tr>
<td>Multi-Queue</td>
<td>100</td>
</tr>
<tr>
<td>Configuring the NAT Policy</td>
<td>102</td>
</tr>
<tr>
<td>Translating IP Addresses</td>
<td>102</td>
</tr>
<tr>
<td>Using Hide NAT</td>
<td>103</td>
</tr>
<tr>
<td>Sample NAT Deployments</td>
<td>103</td>
</tr>
<tr>
<td>NAT Rule Base</td>
<td>105</td>
</tr>
<tr>
<td>Automatic and Manual NAT Rules</td>
<td>105</td>
</tr>
<tr>
<td>Using Automatic Rules</td>
<td>105</td>
</tr>
<tr>
<td>Order of NAT Rule Enforcement</td>
<td>106</td>
</tr>
<tr>
<td>Sample Automatic Rules</td>
<td>106</td>
</tr>
<tr>
<td>Configuring Static and Hide NAT</td>
<td>107</td>
</tr>
<tr>
<td>Enabling Automatic NAT</td>
<td>107</td>
</tr>
<tr>
<td>Automatic Hide NAT to External Networks</td>
<td>108</td>
</tr>
</tbody>
</table>
Enabling Manual NAT .......................................................... 109
Sample Deployment (Static and Hide NAT) ................................ 110
Sample Deployment (Manual Rules for Port Translation) ......... 111
Advanced NAT Settings .......................................................... 113
Deployment Configurations ..................................................... 113
Connecting Translated Objects on Different Interfaces .......... 114
Internal Communication with Overlapping Addresses .......... 114
Security Management Behind NAT ........................................ 117
IP Pool NAT ........................................................................ 118
Monitoring and Logging .......................................................... 123
Monitoring Important Events with SmartEvent ................. 123
Enabling SmartEvent .......................................................... 124
Creating Reports ................................................................ 124
Sample Application Control and URL Filtering Event Analysis .. 125
Monitoring Traffic and Connections with SmartLog ............. 126
Enabling SmartLog .............................................................. 127
Sample Log Analysis ............................................................ 128
LTE .................................................................................. 129
Configuring Fragmentation for IPSec Traffic ....................... 129
Configuring Subnet Range Selection for Quick Mode IDs .......... 130
Configuring Alternate CRL Distribution Points ....................... 130
Configuring Fail Open When CRL is Unavailable .................. 130
Configuring Persistent VPN Kernel Parameters ..................... 131
Disabling IKEv2 Traffic Selector Narrowing ......................... 131
Configuring the GTP Signaling Rate Limit ......................... 131
Configuring GTPv2 Support ................................................ 132
Configuring SCTP Inspection ............................................ 133
Configuring SCTP Acceleration ........................................ 134
Configuring SCTP NAT ..................................................... 135
Configuring GSN Handover Group Limits ......................... 135
Monitoring GSN Handover Group Limits ......................... 135
Deactivating Session Hijacking Protection ......................... 136
Using Diameter Services in Rules ...................................... 136
Creating Diameter SCTP Services ...................................... 137
Creating Diameter TCP Services ...................................... 138
Creating Diameter Applications ...................................... 139
Creating Diameter Application Commands ....................... 140
Blocking Specified Application Commands ...................... 141
Sending Check Point Logs to a Syslog Server .................... 141
Defining Syslog Servers .................................................. 141
Configuring Gateways to Send Logs to Syslog Servers .......... 142
Enabling Syslog in Kernel ................................................. 142
Verification ........................................................................ 143
Configuring CGNAT ........................................................ 143
CGNAT Rule Notes .......................................................... 144
Tracking CGNAT Rule Activity ......................................... 144
Configuring Stateful NAT64 .............................................. 144
Defining a NAT64 Rule .................................................... 145
Other Settings ................................................................. 145
Gateway Configuration ..................................................... 145
Logging ........................................................................ 146
**Terms**

**Anti-Bot**
1. 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.

**APP Wiki**
A searchable application library, for Check Point Application Control and URL Filtering, with details about known Web applications and social networking widgets. (Also: AppWiki)

**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**

**CSCF**
Call Session Control Function. A set of roles for SIP servers or proxies that handle SIP signal packets in the IP Multimedia Subsystem (IMS).

**DBedit**
A CLI tool that lets administrators make changes to objects in the Check Point databases. We recommend that administrators use the GuiDBedit tool instead of dbedit when not using scripts.

**Diameter**
An authentication, authorization and accounting protocol that has many features not included in the legacy RADIUS protocol.

**Diameter Application**
An extension to the Diameter base protocol (as defined in RFC6733). Each application contains one or more commands and/or attributes. Applications are typically associated with an RFC.

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

**DPD**
Dead Peer Detection. A methodology for the detection of a failed IKE peer. It can reclaim lost resources when a peer fails or trigger an IKE peer failover.

**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.

**GGSN**
Gateway GPRS Support Node. The main component of a GPRS network that is responsible for communication between the GPRS network and external, packet-switched networks, such as the Internet.
**GPRS**
General Packet Radio Service. A packet-oriented, mobile data service that works over Global System for Mobile Communication (GSM) networks.

**GSM**
Global System for Mobile Communications. An international standard that defines protocols for second generation digital cellular networks used by mobile phones.

**GTP**
GPRS Tunneling Protocol. A set of IP-based communication protocols that handle GPRS traffic over GSM, UMTS and LTE networks.

**GuiDBedit**
A graphical interface tool for administrators to change objects in Check Point databases.

**HSPA**
High Speed Packet Access. An improved third generation mobile communication protocol that significantly enhances data transfer. It is a combination of two protocols:
- HSUPA - High Speed Uplink Packet Access
- HSDPA - High Speed Downlink Packet Access

**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.

**IPv4 embedded IPv6 address**
An IPv6 address where the rightmost 32 bits are a valid IPv4 address.

**LTE**
Long Term Evolution. A fourth generation communication standard for high-speed wireless communication for mobile phone and data terminals. It is based on GSM and UMTS/HSPA network technologies.

**PDP**

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

**PLMN**
Public Land Mobile Network. A network established and operated by a recognized operating agency to supply land/mobile telephony and data services.

**PSWT**
Public Switched Telephone Network. A collection of public circuit-switched telephone network, including telephone lines, fixed lines, microwave transmission links, cellular networks, and satellite communication.

**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.
SA
Security Association. A VPN tunnel where all hosts on one or more subnets are associated with the tunnel. By default, Check Point VPN tunnels are created between subnets, rather than hosts.

SCTP

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

Security Management Server
The application that manages, 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 through the use of packet inspection.

SGSN
Serving GPRS Support Node. The component of a GPRS network that is responsible for delivery of data packets to and from mobile stations in its geographical service area.

SIP
Session Initiation Protocol. A signaling protocol used for controlling multimedia communication sessions, such as voice and video calls over an IP network.

SmartDashboard
A Check Point client used to create and manage the security policy.

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.

UTMS
Check Point Firewall Security Solution

In This Section:

- Overview of Firewall Features ................................................................. 14
- Licenses ...................................................................................................... 16
- How to Use this Guide ............................................................................ 16
- SmartDashboard Toolbar ........................................................................ 18

Overview of Firewall Features

Firewalls control the traffic between the internal and external networks and are the core of a strong network security policy. Check Point Software Blades are a set of security features that makes sure that the Security Gateway or Security Management Server gives the correct functionality and performance. The Check Point Firewall is part of the Software Blade architecture that supplies “next-generation” firewall features, including:

- VPN and mobile device connectivity
- Identity and computer awareness
- Internet access and filtering
- Application control
- Intrusion and threat prevention
- Data Loss Prevention

Components of the Check Point Solution
Check Point Firewall Security Solution

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet and external networks</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>SmartDashboard</td>
</tr>
<tr>
<td>4</td>
<td>Security Management Server</td>
</tr>
<tr>
<td>5</td>
<td>Internal network</td>
</tr>
</tbody>
</table>

These are the primary components of a Check Point 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.
- **SmartDashboard** - A Check Point client used to create and manage the security policy.

**Dual Stack (IPv4 and IPv6) Network Configuration**

You can easily configure the Firewall to support a dual stack network that uses IPv4 and IPv6 addresses. Configure one or more interfaces with the applicable IPv4 and IPv6 addresses.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Security Gateway for IPv4 network</td>
</tr>
<tr>
<td>5</td>
<td>Security Gateway for IPv6 network</td>
</tr>
<tr>
<td>6</td>
<td>Mobile device [IPv4 traffic]</td>
</tr>
<tr>
<td>7</td>
<td>Mobile devices [IPv6 traffic]</td>
</tr>
</tbody>
</table>

**Note** - For R76 Security Gateways and higher, you can configure the interfaces to use only IPv6 addresses.

**Access Control and the Rule Base**

A primary goal of a firewall is to control access and traffic to and from the internal and external networks. The Firewall lets system administrators securely control access to computers, clients, servers and applications. The Firewall Rule Base defines the quality of the access control and network performance. Rules that are designed correctly make sure that a network:

- Only allows authorized connections and prevents vulnerabilities in a network
- Gives authorized users access to the correct internal networks
- Optimizes network performance and efficiently inspects connections

**Licenses**

Some LTE features require special licenses installed on the Security Gateways. The management server does not require special licenses.

- GTP features require a Carrier license, or the earlier GX/GTP license.
- CGNAT requires the Carrier license.
- SCTP and Diameter inspection require the Carrier license.

If there is no Carrier license on the Security Gateway, you cannot install a policy that has these rules:

- CGNAT rules
- Rules with SCTP or Diameter services
- Rules with **Service = Any** and **Match for any attribute** is enabled for an SCTP service.

**Notes**

- Services defined in **Services > Other** do not require a Carrier license.
- SCTP Connections matching **Other** services are not inspected.

**How to Use this Guide**

When you configure a Firewall, it is necessary that you understand how it is connected to the other Software Blades. For example, you must add a rule for the Firewall to allow remote users to connect to the internal network. In addition, you can enable Software Blades to supply advanced protection for the network, such as IPS and Anti-Bot.
Some of the sections in this guide tell you how to enable a sample configuration of a Software Blade. Make sure that you read the applicable Administration Guide for the Software Blade before you configure the feature for a production environment. Each section also explains rules that you must add to the Firewall Rule Base to complete the configuration for that feature.

**Software Blades in this Guide**

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Creating a Strong Firewall Security Policy (on page 19)</td>
</tr>
<tr>
<td></td>
<td>Configuring the NAT Policy (on page 102)</td>
</tr>
<tr>
<td>Mobile Access</td>
<td>Remote Access to the Network (on page 29)</td>
</tr>
<tr>
<td>IPsec VPN</td>
<td>Creating VPN Policies (on page 42)</td>
</tr>
<tr>
<td>Identity Awareness</td>
<td>Adding Users to the Security Policy (on page 50)</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Defining an Internet Access Policy (on page 62)</td>
</tr>
<tr>
<td>Application Control</td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td>Defending against Network Intrusions (on page 74)</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td></td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>Threat Prevention Policies (on page 80)</td>
</tr>
<tr>
<td>Anti-Spam</td>
<td></td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>Securing Data (on page 86)</td>
</tr>
<tr>
<td>Advanced Networking &amp; Clustering</td>
<td>Maximizing Network Performance (on page 98)</td>
</tr>
</tbody>
</table>
### SmartDashboard Toolbar

You can use the SmartDashboard toolbar to do these actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="" alt="Menu Icon" /></td>
<td>Open the SmartDashboard menu. When instructed to select Manage &gt; Users and Administrators, click this button to open the Manage menu and then select the Users and Administrators option.</td>
</tr>
<tr>
<td><img src="" alt="Save Icon" /></td>
<td>Save current policy and all system objects.</td>
</tr>
<tr>
<td><img src="" alt="Folder Icon" /></td>
<td>Open a policy package, which is a collection of Policies saved together with the same name.</td>
</tr>
<tr>
<td><img src="" alt="Refresh Icon" /></td>
<td>Refresh policy from the Security Management Server.</td>
</tr>
<tr>
<td><img src="" alt="Database Icon" /></td>
<td>Open the Database Revision Control window.</td>
</tr>
<tr>
<td><img src="" alt="Properties Icon" /></td>
<td>Change global properties.</td>
</tr>
<tr>
<td><img src="" alt="Verify Icon" /></td>
<td>Verify Rule Base consistency.</td>
</tr>
<tr>
<td><img src="" alt="Install Icon" /></td>
<td>Install the policy on Security Gateways or VSX Gateways.</td>
</tr>
<tr>
<td><img src="" alt="SmartConsole Icon" /></td>
<td>Open SmartConsole.</td>
</tr>
</tbody>
</table>
Creating a Strong Firewall Security Policy

In This Section:

- Using the Firewall Rule Base
- Creating a Secure Firewall Rule Base
- Defining Security Zones
- Preventing IP Spoofing
- Analyzing the Rule Base [Hit Count]

Using the Firewall Rule Base

The firewall is the core of a well-defined network security policy. The goal of the Check Point Firewall Rule Base is to create rules that only allow the specified connections.

Managing the Firewall Rule Base

Use SmartDashboard to easily create and configure Firewall rules for a strong security policy.

These are the fields that manage the rules for the Firewall security policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the Firewall Rule Base. Implied rules do not have a number.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of connections that match this rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that starts the connection.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that completes the connection.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Definitions of the allowed or blocked traffic between VPN sites.</td>
</tr>
<tr>
<td>Service</td>
<td>Type of network service that is allowed or blocked.</td>
</tr>
<tr>
<td>Action</td>
<td>Firewall action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the rule(s) of the security policy. The Policy Targets option installs the rule(s) on all Security Gateways.</td>
</tr>
<tr>
<td>Time</td>
<td>Time period that the Firewall enforces this rule.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that lets you summarize the rule.</td>
</tr>
</tbody>
</table>

#### Note
The X11 (X Window System Version 11) graphics display system is the standard graphics system for the Unix environment. To enable X11, create a specific rule that allows the X11 service. If you select Any as the Source or Destination, the X11 service is not included.

### Explicit and Implied Rules

These are the types of rules in the Rule Base:

- Explicit rules - Rules that you create to configure which connections the Firewall allows
- Implied rules - Rules that are based on settings in the Global Properties menu

Implied rules allow connections for different services that the Security Gateway uses. For example, the Accept Control Connections option allows packets that control these services:

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

#### To show the implied rules in the Policy window:

1. Make sure there is at least one rule in the Rule Base.
2. Click View > Implied Rules.
   The Policy window in the Firewall tab shows the Rule Base with the explicit and implied rules.

#### To configure the implied rules:

1. Click Policy > Global Properties.
2. From the navigation tree, click Firewall.
3. Select a rule to enable it, or clear a rule to disable it.
4. For the enabled rules, select the position of the rules in the Rule Base ("Order of Rule Enforcement" on page 21).
5. Click OK and install the policy.
Order of Rule Enforcement

The Firewall inspects connections and enforces the Rule Base in a sequential manner. The Firewall inspects each connection that comes to the network and compares the data (source, destination, service, etc.) to the first rule. If the connection matches the rule, the Firewall applies the action of that rule. If the connection does not match the rule, the Firewall continues with the next rule in the Rule Base.

```
<table>
<thead>
<tr>
<th>Request to open connection</th>
<th>Firewall compares connection data to rule</th>
<th>Does the data match the rule?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>
```

*Note* - We recommend that you create a Cleanup rule as the final rule in the Rule Base. This rule matches all connections and drops them.

Make sure that you understand the importance of the order of rule enforcement to maximize the security of the Firewall. The Firewall always enforces the *first* rule that matches a connection. It does not enforce later rules that can be more applicable.

This is the order that rules are enforced:

1. **First Implied Rule**: You cannot edit or delete this rule and no explicit rules can be placed before it.
2. **Explicit Rules**: These are rules that you create.
3. **Before Last Implied Rules**: These implied rules are applied before the last explicit rule.
4. **Last Explicit Rule**: We recommend that you use the Cleanup rule as the last explicit rule.
5. **Last Implied Rules**: Implied rules that are configured as *Last* in Global Properties.
6. **Implied Drop Rule**: Drops all packets without logging.

*Note* - If you use the Cleanup rule as the last explicit rule, the *Last implied rule* and the *Implied drop rule* are not enforced.

Creating a Secure Firewall Rule Base

**Basic Rules**

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.

There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.
Sample Firewall Rule Base

This table shows a sample Firewall Rule Base for a typical security policy. (The Hits and VPN columns are not shown.)

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stealth</td>
<td>NOT Internal</td>
<td>GW-group</td>
<td>Any</td>
<td>Drop</td>
<td>Alert</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>2</td>
<td>Critical subnet</td>
<td>Internal</td>
<td>Finance HR R&amp;D</td>
<td>Any</td>
<td>Accept</td>
<td>Log</td>
<td>CorpGW</td>
</tr>
<tr>
<td>3</td>
<td>Tech support</td>
<td>TechSupport</td>
<td>Remotel-web</td>
<td>HTTP</td>
<td>Accept</td>
<td>Alert</td>
<td>Remotel1GW</td>
</tr>
<tr>
<td>4</td>
<td>DNS server</td>
<td>Any</td>
<td>DNS</td>
<td>Domain UDP</td>
<td>Accept</td>
<td>None</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>5</td>
<td>Mail and Web servers</td>
<td>Any</td>
<td>DMZ</td>
<td>HTTP HTTPS SMTP</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>6</td>
<td>SMTP</td>
<td>Mail</td>
<td>NOT Internal net group</td>
<td>SMTP</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>7</td>
<td>DMZ &amp; Internet</td>
<td>IntGroup</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>8</td>
<td>Clean up rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

1. **Stealth** - All traffic that is NOT from the internal company network to one of the Security Gateways is dropped. When a connection matches the Stealth rule, an alert window opens in SmartView Monitor.

2. **Critical subnet** - Traffic from the internal network to the specified resources is logged. This rule defines three subnets as critical resources: Finance, HR, and RnD.

3. **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.

4. **DNS server** - Allows UDP traffic to the external DNS server. This traffic is not logged.

5. **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.

6. **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.

7. **DMZ and Internet** - Allows traffic from the internal network to the DMZ and Internet.

8. **Clean up rule** - Drops all traffic. All traffic that is allowed matched one of the earlier rules.

Defining Security Zones

Networks use different security zones to protect very important resources and to defend against malware. Create rules that allow only the applicable traffic in and out of a security zone. Make sure that there are different rules in the Firewall Rule Base that define traffic to and from the security zones. These are the key elements that define security zones:

- **External network** - Insecure data, such as the Internet
- **Internal network** - Company data that is only used by trusted and authenticated users
- **Perimeter** - The border between the internal and external networks.
- **DMZ** - Company servers that can be accessed from insecure sources, such as the Internet
Perimeter

The Firewall on the perimeter of the network is responsible for all the incoming and outgoing traffic. These are some of the connections that are usually allowed by a Firewall on the perimeter:

- Outgoing connections to the Internet
- Connections to the DNS server
- Specified external connections
- Connections to servers in the DMZ
- Connections from the internal network to the internal network
- VPN connections

DMZ

Servers that are accessed by the Internet are usually located in a DMZ (demilitarized zone). The DMZ makes sure that these servers cannot connect to the internal network. Make sure that the Rule Base contains rules for DMZ traffic. For example, these are rules for a web server in the DMZ:

- A rule that allows HTTP and HTTPS traffic to the DMZ network object
- A rule that allows traffic from the internal network group object to any destination (the destination includes the DMZ)

Preventing IP Spoofing

Attacks use IP spoofing to make the IP address of a packet appear to be from a trusted source. This can bypass the Firewall to introduce malicious content and actions (malware and bot downloads, DoS attacks, unauthorized access, and so on) to your network.

Anti-Spoofing detects if a packet with an IP address that is, according to the topology, behind one interface, actually arrives from a different interface. For example, if a packet from an external network has an internal IP address, Anti-Spoofing blocks the packet.
Creating a Strong Firewall Security Policy

### Item Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Interface IF1</td>
</tr>
<tr>
<td>2</td>
<td>Interface IF2</td>
</tr>
<tr>
<td>3</td>
<td>Interface IF3</td>
</tr>
<tr>
<td>4</td>
<td>Interface IF4</td>
</tr>
<tr>
<td>5</td>
<td>Alaska_LAN</td>
</tr>
<tr>
<td>6</td>
<td>Florida_LAN</td>
</tr>
<tr>
<td>7</td>
<td>Alaska_RND_LAN</td>
</tr>
<tr>
<td>8</td>
<td>Internet</td>
</tr>
<tr>
<td>9</td>
<td>Alaska_GW</td>
</tr>
<tr>
<td>10</td>
<td>Alaska_RND_GW</td>
</tr>
</tbody>
</table>

For the Alaska_GW, the Firewall makes sure that:

- All incoming packets to IF1 come from the Internet.
- All incoming packets to IF2 come from Alaska_LAN or Alaska_RND_LAN or Florida_LAN.

For the Alaska_RND_GW, the Firewall makes sure that:

- All incoming packets to IF3 come from Alaska_LAN, Florida_LAN or the Internet.
- All incoming packets to IF4 come from Alaska_RND_LAN.

When you configure Anti-Spoofing for a Security Gateway, specify if the interfaces go to the Internet (External) or an internal network (Internal).

### Configuring Anti-Spoofing

Use the Topology page to configure Anti-Spoofing for the external and internal interfaces on the Security Gateway. Configure Anti-Spoofing protection on all the interfaces of the Security Gateway, including internal interfaces.

SmartDashboard attempts to automatically retrieve the topology from the Security Gateway. If it cannot retrieve the topology information, make sure that:

- The details in the Security Gateway General Properties window are correct.
- The Security Gateway, the Security Management Server, and the SmartDashboard can communicate with each other.

When you configure an internal interface, select the option for the IP addresses that are connected to the interface. These are the network options:

- **Not Defined** - All IP addresses are considered as part of the internal network that connects to this internal interface.
- **Network defined by the interface IP and Net Mask** - There is only one network that connects to this internal interface.
- **Specific** - There is more than one network that connects to this internal interface. Select the group network object that contains all the appropriate networks.

**To configure Anti-Spoofing for an interface:**

1. In SmartDashboard, from the **Network Objects** tree, double-click the Security Gateway. The General Properties window opens.
2. From the navigation tree, click **Topology**.
3. Click **Get > Interfaces**.
4. Click **Accept**.

5. Select the interface that connects to the Internet and click **Edit**. The **Interface Properties** window opens.

6. Click the **Topology** tab.

7. Select **External** or **Internal**.

8. For **Internal** interfaces, do these steps:
   a) Select the option for the network **IP Addresses behind this interface**.
   b) If the internal interface connects to a DMZ, select **Interface leads to DMZ**.

9. Select **Perform Anti-Spoofing based on interface topology**.
10. Select an **Anti-Spoofing action**.
   - **Prevent** - Drops spoofed packets.
   - **Detect** - Allows spoofed packets.

   We recommend that you use the **Detect** option to monitor traffic. You can use it with a **Spoof Tracking** option to learn about the network topology without rejecting packets.

11. **Optional for External Interfaces**: Configure the IP addresses that are not included in Anti-Spoofing ("Excluding Specific Internal Addresses" on page 26).
   a) Select **Don't check packets from**.
   b) Click the field, and select the Group or Network object that you are not including in Anti-Spoofing.

      You can click **New** to create a new Group or Network object.

12. From **Spoof Tracking**, select the tracking action that is done when Anti-Spoofing is detected.
13. Click **OK** and configure Anti-Spoofing for all the interfaces on the Security Gateway.
14. Click **OK** and install the policy.

---

**Excluding Specific Internal Addresses**

In some configurations, the Firewall must allow connections with an internal IP address from an external source. For example, an external application can assign internal IP addresses to external clients. You can configure the Anti-Spoofing protection on the external interfaces to ignore connections from these IP addresses. The Firewall allows these connections and does not inspect them.

---

**Analyzing the Rule Base (Hit Count)**

Use the Hit Count feature to track the number of connections that each rule matches. 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 Firewall 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**.

You can 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 Firewall performance - You can move a rule that has a high hit count to a higher position in the Rule Base
- Better understand the behavior of the security Policy
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. From the Policy menu, select 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 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.
4. Click OK and then 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 and then 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 (versions before R75.40)
  - 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)
<table>
<thead>
<tr>
<th>Hit Count Level</th>
<th>Icon</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td><img src="image" alt="Zero Icon" /></td>
<td>0 hits</td>
</tr>
<tr>
<td>Low</td>
<td><img src="image" alt="Low Icon" /></td>
<td>Less than 10 percent of the hit count range</td>
</tr>
<tr>
<td>Medium</td>
<td><img src="image" alt="Medium Icon" /></td>
<td>Between 10 - 70 percent of the hit count range</td>
</tr>
<tr>
<td>High</td>
<td><img src="image" alt="High Icon" /></td>
<td>Between 70 - 90 percent of the hit count range</td>
</tr>
<tr>
<td>Very High</td>
<td><img src="image" alt="Very High Icon" /></td>
<td>Above 90 percent of the hit count range</td>
</tr>
</tbody>
</table>

To configure the Hit Count display:

1. Right-click the **Hits** column header or the rule number in the row.
2. From the menu, select **Display**.
3. Select one or more options:
   - Percentage
   - Value
   - Level
Remote Access to the Network

Overview

Check Point Mobile Access Software Blade extends the functionality of a Firewall and 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. They can then authenticate with multiple options such as: user name/password, certificates, or SecurID.

SmartDashboard lets you easily create user groups and give the users access to the applicable applications. These are some of the different corporate applications that users can access:

- Web applications - A set of URLs that are accessed with an Internet browser. For example: inventory management or HR management applications.
- File share - A collection of files that are available with a specified protocol, such as SMB for Windows. Users can read, write, and delete files that are stored on the network.
- Citrix clients - Users can connect to internal XenApp servers.
- Web mail services - Mobile Access provides a front end for email servers that support IMAP and SMTP protocols. You can also configure other Web-based mail services, such as OWA (Outlook Web Access) and iNotes (IBM Lotus Domino Web Access).


Check Point Mobile Access Solutions

Check Point Mobile Access has a range of flexible clients and features that let users access internal resources from remote locations. All these solutions include these features:

- Enterprise-grade, secure connectivity to corporate resources
- Strong user authentication
- Granular access control

For more information about the newest versions of Mobile Access solutions and clients, go to sk67820 http://supportcontent.checkpoint.com/solutions?id=sk67820.
Client-Based vs. Clientless

Check Point remote access solutions use IPsec and SSL encryption protocols to create secure connections. All Check Point clients can work through NAT devices, hotspots, and proxies in situations with complex topologies, such as airports or hotels. These are the types of installations for remote access solutions:

- **Client-based** - Client application installed on endpoint computers and devices. Clients are usually installed on a managed device, such as a company-owned computer. The client supplies access to most types of corporate resources according to the access privileges of the user.

- **Clientless** - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.

- **On demand client** - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

Mobile Access Clients

- Capsule Workspace - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.

- Capsule Connect - A full L3 tunnel app that gives users network access to all mobile applications.

- Check Point Mobile for Windows - A Windows IPsec VPN client that supplies secure IPsec VPN connectivity and authentication.

Mobile Access Web Portal

The Mobile Access Portal is a clientless SSL VPN solution that supplies secure access to web-based resources. After users authenticate to the portal, they can access Mobile Access applications such as Outlook Web App and a corporate wiki.

SSL Network Extender

SSL Network Extender is an on-demand SSL VPN client and is installed on the computer or mobile device from an Internet browser. It supplies secure access to internal network resources.

Configuring Remote Access to Network Resources

Sample Mobile Access Workflow

This is a high-level workflow to configure remote access to the internal applications and resources.

1. Use SmartDashboard to enable the Mobile Access Software Blade on the Security Gateway.
2. Follow the steps in the Mobile Access Configuration wizard to configure these settings:
   - Select mobile device access clients
   - Define the Mobile Access portal
Remote Access to the Network

- Define the web applications, for example Outlook Web App
- Connect to the AD server for user information

3. For VPN clients, add Firewall rules to allow the mobile device connections.

4. **Optional**: Distribute client certificates to authenticate the mobile users.
   For R76 and higher, use the Certificate Creation and Distribution Wizard.

5. Users download the Capsule Workspace app.

6. Users open the Capsule Workspace app and enter the Mobile Access Site Name and necessary authentication, such as user name and password.

Sample Mobile Access Deployment

This is a sample deployment of a Mobile Access Security Gateway with an AD and Exchange server in the internal network.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile devices</td>
</tr>
<tr>
<td>2</td>
<td>Mobile Access tunnels</td>
</tr>
<tr>
<td>3</td>
<td>Internet (external networks)</td>
</tr>
</tbody>
</table>

From SmartDashboard, enable Mobile Access

Configure settings in Mobile Access wizard

Add rules for mobile devices to Firewall

Generate a certificate for the clients

Users can access internal resources

Users open app and enter settings

Users download app
Remote Access to the Network

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Mobile Access Security Gateway</td>
</tr>
<tr>
<td>5</td>
<td>Internal network resources, AD and Exchange servers</td>
</tr>
</tbody>
</table>

In this sample Mobile Access deployment, a mobile device uses a Mobile Access tunnel to connect to the internal network. The Mobile Access Security Gateway decrypts the packets and authenticates the user. The connection is allowed and the mobile device connects to the internal network resources.

Using the Mobile Access Configuration Wizard

This procedure describes how to enable and configure the Mobile Access Software Blade on a Security Gateway with the Configuration wizard. For this sample configuration, the AD user group Mobile_Access contains all the users that are allowed to connect to the internal network. The deployment is based on the Sample Mobile Access Deployment (on page 31).

This configuration lets these clients connect to internal resources:
- Android and iOS mobile devices
- Windows and Mac computers
- Internet browsers can open a SSL Network Extender connection to the internal network

To configure Mobile Access:

1. In SmartDashboard, from the Network Objects tree, double-click the Security Gateway. The General Properties window opens.
3. Configure the Security Gateway to allow connections from the Internet and mobile devices. Select these options:
   - Web
   - Mobile Devices - Business Secure Container and VPN Client
   - Desktops - With compliance check
4. Click **Next**.
   The **Web Portal** page opens.
5. Enter the primary URL for the Mobile Access portal. The default is 
   https://<gw_IPv4>/sslvpn
6. Click **Next**.
   The **Applications** page opens.
7. Configure the applications that are shown:
   a) In **Web Applications**, make sure **Demo web application** is selected.
   b) In **Mail/Calendar/Contacts**, enter the domain for the Exchange server and select these options:
      - **Check Point Secure Mail**
      - **ActiveSync Applications**
      - **Outlook Web App**
   The Mobile Access portal shows links to the Demo web and Outlook Web App applications. The client on the mobile device shows links to the other applications.
8. Click **Next**.
   The **Active Directory** page opens.
9. Select the AD domain and enter the user name and password.
10. Click **Connect**.
    The Security Gateway makes sure that it can connect to the AD server.
11. Click **Next**.
    The **Users** page opens.
    Click **Add** and then select the group **Mobile_Access**.
12. Click **Next** and then click **Finish**.
    The **Mobile Access Configuration Wizard** closes.
13. Click **OK**.
    The **Gateway Properties** window closes.

**Allowing Mobile Connections**

The Mobile Access Configuration Wizard enables and configures the Mobile Access Software Blade. It is necessary to add Firewall rules to allow connections from the VPN clients on the computers and devices. Create a Host Node object for the Exchange server, all of the other objects are predefined.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Access</td>
<td>Any</td>
<td>ExchngSrvr</td>
<td>RemoteAccess</td>
<td>HTTP</td>
<td>Accept</td>
<td>MobileAccessGW</td>
<td>Log</td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td>HTTPS Exchange</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All connections from the **RemoteAccess VPN** community to the Exchange server are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and MS Exchange. This rule is installed on Security Gateways in the **MobileAccessGW** group.
Defining Access to Applications

Use the Policy page to define rules that let users access Mobile Access applications. The applications that are selected in the Configuration wizard are automatically added to this page. You can also create and edit the rules that include these SmartDashboard objects:

- Users and user groups
- Mobile Access applications
- Mobile Access Security Gateways

Sample Mobile Access Policy

The Mobile Access rule lets the users in the Mobile_Access AD group access these applications on the Tokyo_Gateway:

- OWA - Outlook Web Access
- Mobile Secure Mail - Capsule Workspace clients can connect to the Exchange mail server to use email applications
- Access_My_PC - Remote Desktop application
- Corporate_Portal - Connect to the internal corporate web portal
- ActiveSync App - Connect to the Exchange mail server to use email applications such as Outlook

Activating Single Sign On

Enable the SSO (Single Sign On) feature to let users authenticate one time for applications that they use during Mobile Access sessions. The credentials that users enter to log in to the Mobile Access portal can be re-used automatically to authenticate to different Mobile Access applications. SSO user credentials are securely stored on the Mobile Access Security Gateway for that session and are used again if users log in from different remote devices. After the session is completed, the credentials are stored in a database file.

By default, SSO is enabled on new Mobile Access applications that use HTTP. Most Web applications authenticate users with specified Web forms. You can configure SSO for an application to use the authentication credentials from the Mobile Access portal. It is not necessary for users to log in again to each application.
To configure SSO:

1. In the **Mobile Access** tab, select **Additional Settings > Single Sign On**. The **Single Sign On** page opens.

2. Select an application and click **Edit**. The application properties window opens and shows the **Single Sign On** page.

3. For Web form applications, do these steps:
   a) In the **Application Single Sign On Method** section, select **Advanced** and click **Edit**. The **Advanced** window opens.
   b) Select **This application reuses the portal credentials. Users are not prompted**.
   c) Click **OK**.
   d) Select **This application uses a Web form to accept credentials from users**.
   e) Click **OK**.

4. Install the policy.

### Connecting to a Citrix Server

**Citrix Services**

The Mobile Access Software Blade integrates the Firewall Citrix clients and services. It is not necessary to use STA (Secure Ticketing Authority) servers in a Mobile Access Security Gateway deployment because Mobile Access uses its own STA engine. You can also use Mobile Access in a deployment with STA and CSG (Citrix Secure Gateway) servers.

The Mobile Access server certificate must use a FQDN (Fully Qualified Domain Name) that is issued to the FQDN of the Mobile Access Security Gateway.
Sample Deployment with Citrix Server

This is a sample deployment of a Mobile Access Security Gateway and a Citrix web server in the DMZ. The Citrix XenApp server is connected to the internal network.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile devices</td>
</tr>
<tr>
<td>2</td>
<td>Mobile Access tunnels</td>
</tr>
<tr>
<td>3</td>
<td>Internet (external networks)</td>
</tr>
<tr>
<td>4</td>
<td>Security Gateway for the internal network</td>
</tr>
<tr>
<td>5</td>
<td>Mobile Access Security Gateway in the DMZ</td>
</tr>
<tr>
<td>6</td>
<td>Citrix web interface</td>
</tr>
<tr>
<td>7</td>
<td>Internal network resources</td>
</tr>
<tr>
<td>8</td>
<td>Citrix XenApp (MetaFrame) server</td>
</tr>
</tbody>
</table>
Configuring Citrix Services for Mobile Access

This procedure describes how to configure Mobile Access to let remote users connect to Citrix applications. The deployment is based on the Sample Deployment with Citrix Server (on page 36).

To configure Citrix services:

1. In the Mobile Access tab, select Endpoint Security on Demand > Applications > Citrix Services.
2. Click New.
   The General Properties page of the Citrix Service window opens.
3. Enter the Name for the Citrix server object.
4. From the navigation tree, click Web Interface.
5. Create a new object for the Citrix web interface server, in Servers, click Manage > New > Host.
   The Host Node window opens.
6. Enter the settings for the Citrix web interface server and the click OK.
7. In Services, select one or more of these services that the Citrix web interface server supports:
   • HTTP
   • HTTPS
8. From the navigation tree, click Link in Portal.
9. Configure the settings for the link to the Citrix services in the Mobile Access portal:
   • Link text - The text that is shown for the Citrix link
   • URL - The URL for the directory or subdirectory of the Citrix application
   • Tooltip - Text that is shown when the user pauses the mouse pointer above the Citrix link
10. From the navigation tree, select Additional Settings > Single Sign On.
11. Enable Single Sign On for Citrix services, select these options:
   • Turn on single Sign On for this application
   • Prompt users for their credentials
12. Click OK.
   The Citrix server object is added to Defined Citrix Services.
13. From the Mobile Access navigation tree, select Policy.
14. Add the Citrix services object to the applicable rules.
   a) Right-click on the Applications cell of a rule and select Add Applications.
   b) Select the Citrix services object.
15. Install the policy.

Compliance Check

The Mobile Access Software Blade lets you use the Endpoint Security on Demand feature to create compliance policies and add more security to the network. Mobile devices and computers are scanned one time to make sure that they are compliant before they can connect to the network.

The compliance scanner is installed on mobile devices and computers with ActiveX (for Internet Explorer on Windows) or Java. The scan starts when the Internet browser tries to open the Mobile Access Portal.
Compliance Policy Rules

The compliance policy is composed of different types of rules. You can configure the security and compliance settings for each rule or use the default settings.

These are the rules for a compliance policy:

- Windows security - Microsoft Windows hotfixes, patches and Service Packs.
- Anti-Spyware protection - Anti-Spyware software.
- Anti-Virus protection - Anti-Virus software version and virus signature files.
- Firewall - Personal firewall software.
- Spyware scan - Action that is done for different types of spyware.
- Custom - Compliance rules for your organization, for example: applications, files, and registry keys.
- OR group - A group of the above rules. An endpoint computer is compliant if it meets one of the rules in the group.

Creating a Compliance Policy

The default setting for Endpoint Security on Demand is that all endpoint computers cannot log in to the Mobile Access portal until they are compliant with the Compliance policy. Use the Policies window to create or edit a Compliance policy.

This procedure shows how to configure a sample policy for company laptop computers.

To create a Compliance policy:

1. In the Mobile Access tab, select Endpoint Security on Demand > Compliance.
2. Click Edit policies.
   The Policies window opens.

3. Click New Policy.
   The Policies > New Policy window opens.
4. Enter the Name and Description for the policy.
5. Click Add.
   The Add Enforcement Rules window opens.
6. Select the rules for the policy.
These are the rules for the sample laptop computer policy:
- Default Windows Security rule
- High security Anti-Spyware applications check
- High security Anti-Virus applications check
- High security spyware scan
- Medium security Firewall applications check

7. Click OK.
The Policies > Edit Policy window shows the rules for the policy.

8. Select Bypass spyware scan.
When this feature is selected, the scan for endpoint computers that are compliant with the Anti-Virus or Anti-Spyware settings is changed. These computers do not scan for spyware when they connect to a Mobile Access Security Gateway.

9. Click OK.
The Policies window opens.

10. Click OK.

Configuring Compliance Settings for a Security Gateway
The Firewall on a Mobile Access Security Gateway only allows access to endpoint computers that are compliant with the Compliance policy.

This procedure shows how to configure the Laptop Computer policy ("Compliance Policy Rules" on page 38) for a Security Gateway.
To configure the Compliance settings:

1. In the **Mobile Access** tab, select **Endpoint Security on Demand > Compliance**.

2. Select the Security Gateway and click **Edit**. The **Compliance** page of the Security Gateway properties window opens.

3. Select **Scan endpoint machine when user connects**.

4. Click **Threshold policy** and from the drop-down menu select **Laptop Computer**.

5. Click **OK**.


**Using Secure Workspace**

Secure Workspace is a security solution that allows remote users to connect to enterprise network resources safely and securely. The Secure Workspace virtual workspace provides a secure environment on endpoint computers that is segregated from the “real” workspace. Users can only send data from this secure environment through the Mobile Access portal. Secure Workspace users can only access permitted applications, files, and other resources from the virtual workspace.

Secure Workspace creates an encrypted folder on the computer called **My Secured Documents** and can be accessed from the virtual desktop. This folder contains temporary user files. When the session terminates, Secure Workspace deletes this folder and all other session data.

To enable Secure Workspace on a Mobile Access Security Gateway:

1. In the **Mobile Access** tab, select **Endpoint Security on Demand > Secure Workspace**.
2. Select the Security Gateway and click **Edit**.
   The **Check Point Secure Workspace** page of the Security Gateway properties window opens.
3. Select **This gateway supports access to applications from within Check Point Secure Workspace**.
4. Click **OK** and then install the policy.
Creating VPN Policies

In This Section:

Overview ..........................................................................................................................42
Using Site to Site VPN ..................................................................................................45
Using Remote Access VPN...........................................................................................48

Overview

The IPsec VPN Software Blade lets the Firewall encrypt and decrypt traffic to and from external networks and clients. Use SmartDashboard to easily configure VPN connections between Security Gateways and remote devices. You can configure Star and Mesh topologies for large-scale VPN networks that 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.

For more about using IPsec VPN, see the R77 VPN Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=24849.

Site to Site VPN

The basis of Site to Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.
Creating VPN Policies

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>VPN tunnel</td>
</tr>
<tr>
<td>3</td>
<td>Internal network in VPN domain</td>
</tr>
<tr>
<td>4</td>
<td>Host 1</td>
</tr>
<tr>
<td>5</td>
<td>Host 6</td>
</tr>
</tbody>
</table>

In this sample VPN deployment, Host 1 and Host 6 securely send data to each other. The Firewalls do IKE negotiation and create a VPN tunnel. They use the IPsec protocol to encrypt and decrypt data that is sent between Host 1 and Host 6.

**VPN Workflow**

Host 1 sends packet to Host 6

Firewalls A & B create VPN tunnel

Firewall A encrypts data

Host 6 receives unencrypted data

Firewall B decrypts data

Encrypted data is sent through VPN tunnel

**VPN Communities**

A VPN Domain is a collection of internal networks that use Security Gateways to send and receive VPN traffic. Define the resources that are included in the VPN Domain for each Security Gateway. Then join the Security Gateways into a VPN community - collection of VPN tunnels and their attributes. Network resources of different VPN Domains can securely communicate with each other through VPN tunnels that terminate at the Security Gateways in the VPN communities.

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN tunnels between each pair of Security Gateway. In a Star community, each satellite Security Gateway has a VPN tunnel to the central Security Gateway, but not to other Security Gateways in the community.
Creating VPN Policies

Firewall Administration Guide R77 Versions   |   44

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway. For Star topology, the central Security Gateway.</td>
</tr>
<tr>
<td>2</td>
<td>For Star topology, satellite Security Gateways.</td>
</tr>
</tbody>
</table>

**Sample Combination VPN Community**

![Diagram of Sample Combination VPN Community]

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>London Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>New York Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>London - New York Mesh community</td>
</tr>
<tr>
<td>4</td>
<td>London company partner (external network)</td>
</tr>
<tr>
<td>5</td>
<td>London Star community</td>
</tr>
<tr>
<td>6</td>
<td>New York company partner (external network)</td>
</tr>
<tr>
<td>7</td>
<td>New York Star community</td>
</tr>
</tbody>
</table>

This deployment is composed of a Mesh community for London and New York Security Gateways that share internal networks. The Security Gateways for external networks of company partners do not have access to the London and New York internal networks. The Star VPN communities let the company partners access the internal networks.

**Routing VPN Traffic**

Configure the Security Gateway to route VPN traffic based on VPN domains or based on the routing settings of the operating system.

**Note** - For each VPN gateway, you must configure an existing gateway as a default gateway.
Domain Based VPN

The VPN traffic is routed according to the VPN domains that are defined in SmartDashboard. Use domain based routing to let satellite Security Gateways send VPN traffic to each other. The center Security Gateway creates VPN tunnels to each satellite and the traffic is routed to the correct VPN domain.

Route Based VPN

VPN traffic is routed according to the routing settings (static or dynamic) of the Security Gateway operating system. The Security Gateway uses a VTI (VPN Tunnel Interface) to send the VPN traffic as if it were a physical interface. The VTIs of Security Gateways in a VPN community connect and can support dynamic routing protocols.

Granular Routing Control

The Link Selection feature gives you granular control of the VPN traffic in the network. Use this feature to enable the Security Gateway to:

- Find the best possible route for VPN traffic
- Select the interfaces that are used for VPN traffic to internal and external networks
- Configure the IP addresses that are used for VPN traffic
- Use route probing to select available VPN tunnels
- Use Load Sharing for Link Selection to equally distribute VPN traffic to VPN tunnels

Remote Access VPN

If employees remotely access sensitive information from different locations and devices, system administrators must make sure that this access does not become a security vulnerability. Check Point’s Remote Access VPN solutions let you create a VPN tunnel between a remote user and the internal network. The Mobile Access Software Blade ("Remote Access to the Network" on page 29) extends the functionality of Remote Access solutions to include many clients and deployments.

Using Site to Site VPN

Sample Star Deployment

This section explains how to configure a VPN star community. This deployment lets the satellite Security Gateways connect to the internal network of the central Security Gateway. The internal network object is named: Internal-network.
To create a new VPN Star Community:

1. In the IPsec VPN tab, select Communities.

2. Click New > Star Community.
   The General page of the Star Community Properties window opens.

3. Enter the name for the community.

4. From the navigation tree, select Encryption.

5. Configure the VPN encryption methods and algorithms for the VPN community.

6. Click OK.

To configure star VPN for the Security Gateways:

1. Double-click the Security Gateway.
   The Gateway Properties window opens.

2. In Network Security, select IPsec VPN.

3. From the navigation tree, click Topology.

4. In the VPN Domain section:
   • For the central Security Gateway, click Manually defined and select the Internal-network object.
   • For a satellite Security Gateway, select All IP addresses.

5. From the navigation tree, click IPsec VPN.

6. Configure the Security Gateway as a member of a VPN star community.
   a) In the This Security Gateway participates in the following VPN Communities section, click Add.
      The Add this Gateway to Community window opens.
   b) Select the VPN Community and click OK.
c) Configure the Security Gateway as a hub or a spoke.
   - For the center, select **Center Gateways**.
   - For the satellites, select **Satellite Gateways**.

d) Click **Add**.

e) Click **OK**.

7. Do these steps for all the Security Gateways for the VPN community.

**Allowing VPN Connections**

When you create a VPN connection between Security Gateways, add Firewall rules to allow the VPN traffic. Use the VPN Community objects in the VPN column of the Firewall Rule Base to define access control for VPN connections in the network.

**Allowing All VPN Traffic**

Use the **Allow All Encrypted traffic** feature to configure the Firewall to allow all VPN traffic to the internal networks for the VPN communities. It is not necessary to add rules to the Firewall Rule Base that allow the VPN traffic for the specified VPN communities.

SmartDashboard adds this automatic rule to the top of the Rule Base:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>NOT Member Gateways</td>
<td>&lt;VPN community&gt; Encrypted Services</td>
<td>Accept</td>
<td>Log</td>
<td>&lt;VPN gateways&gt;</td>
<td></td>
</tr>
</tbody>
</table>

This automatic rule allows all encrypted packets that are sent between hosts or clients in the specified VPN community. Traffic that is sent to the Security Gateways in the VPN community is dropped. The rule is installed on all Security Gateways in the VPN communities.

**Note** - This automatic rule can apply to more than one VPN community.

**Sample VPN Firewall Rules**

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Any</td>
<td>NOT Member Gateways</td>
<td>BranchOffices</td>
<td>Encrypted Services</td>
<td>BranchOffices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LondonOffices</td>
<td></td>
<td>LondonOffices</td>
</tr>
<tr>
<td>2</td>
<td>Site to site VPN</td>
<td>Any</td>
<td>Any</td>
<td>All_GwToGw</td>
<td>FTP-port HTTP</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTPS SMTP</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Remote access</td>
<td>Any</td>
<td>Any</td>
<td>RemoteAccess</td>
<td>HTTP HTTPS</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IMAP</td>
<td></td>
</tr>
</tbody>
</table>
The first rule is the automatic rule for the **Accept All Encrypted Traffic** feature. The Firewalls for the Security Gateways in the BranchOffices and LondonOffices VPN communities allow all VPN traffic from hosts in clients in these communities. Traffic to the Security Gateways is dropped. This rule is installed on all Security Gateways in these communities.

2. **Site to site VPN** - Connections between hosts in the VPN domains of all Site to Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.

3. **Remote access** - Connections between hosts in the VPN domains of RemoteAccess VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

**Using Remote Access VPN**

This section explains how to use a VPN tunnel to connect a client-based remote computer to an internal network. For more about using Mobile Access to connect remote devices to internal resources, see Remote Access to the Network (on page 29).

- **Note** - For each VPN gateway, you must configure an existing gateway as a default gateway.

**VPN Connectivity Modes**

The IPsec VPN Software Blade lets the Firewall overcome connectivity challenges for remote clients. Use VPN connectivity modes to make sure that remote users can connect to the VPN tunnels. These are some examples of connectivity challenges:

- The IP addresses of a remote access client might be unknown
- The remote access client can be connected to a hotel LAN with internal IP addresses
- It is necessary for the remote client to use protocols that are not supported

**Office Mode**

Remote users can be assigned the same or non-routable IP addresses from the local ISP. Office Mode solves these routing problems and encapsulates the IP packets with an available IP address from the internal network. Remote users can send traffic as if they are in the office and do not have VPN routing problems.

**Visitor Mode**

Remote users can be restricted to use HTTP and HTTPS traffic only. Visitor Mode lets these users tunnel all protocols with a regular TCP connection on port 443.

**Sample Remote Access VPN Workflow**

Use SmartDashboard to enable and configure the Security Gateway for remote access VPN connections. Then add the remote user information to the Security Management Server: create and configure an LDAP Account Unit or enter the information in the SmartDashboard user database. You can also configure the Firewall to authenticate the remote users. Define the Firewall access control and encryption rules. Create the LDAP group or user group object that is used for the Firewall rules. Then create and configure the encryption settings for the VPN community object. Add the access rules to the Firewall Rule Base to allow VPN traffic to the internal networks.
Enable remote access VPN

Configure LDAP Account Unit

Configure user authentication

Create LDAP user group object

Create VPN Community

Configure rules for VPN access in Firewall Rule Base

Install policy

Manage Users? Smart Dashboard Configure users in SmartDashboard database

LDAP

Configure LDAP

Create user group object

Configure user authentication

Configure user authentication
Adding Users to the Security Policy

In This Section:

Using Identity Awareness ................................................................. 50
Using User Directory ...................................................................... 55
Adding Users to the Rule Base ......................................................... 61

Using Identity Awareness

The Identity Awareness Software Blade lets you configure the Firewall to enforce access control for individual users and groups. You can use Identity Sources to get information about users and groups to create flexibility and additional security for the Rule Base. Identity Awareness lets you create rules that are for the specified users for these Rule Bases:

- Firewall
- URL Filtering and Application Control
- DLP
- Anti-Bot

For more about using Identity Awareness, see the R77 Identity Awareness Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=24805.

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:

- **AD Query** - Seamlessly queries the AD (Active Directory) servers to get user information.
- **Browser-Based Authentication** - Uses a Captive Portal to authenticate users.
- **Identity Agent** - Client that is installed on endpoint computers connects to a Security Gateway and authenticates users.
- **Terminal Servers Identity Agent** - An agent on a Terminal or Citrix server connects to a Security Gateway to get user information.
- **Remote Access Devices** - Use Identity Awareness with the Mobile Access and VPN Software Blades (Office Mode only) to authenticate users that connect from a remote device.

**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 Firewall identifies the user based on the AD security event log. The user sends traffic that matches an Identity Awareness rule in the security policy. The Firewall can enforce the user-based rule on the traffic.
**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.

**Enabling Identity Awareness**

There is an Identity Awareness configuration wizard in SmartDashboard 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 Wizard**

The Identity Awareness Configuration wizard configures how the Security Gateway gets information about users and computers.

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

To use the configuration wizard:

1. From the **Network Objects** tree, double-click the Security Gateway. The **Gateway Properties** window opens.
2. From the navigation tree, click **General Properties**.
3. From the **Network Security** tab, select **Identity Awareness**.
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 Password. Make sure that the AD account has domain administrator privileges.

6. Click Connect. The Successfully connected message is shown.

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 and then 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. From the Network Objects tree, double-click the Security Gateway. The Gateway Properties window opens.

2. From the navigation tree, click Identity Awareness.

3. Select or clear Remote Access.

4. Click OK and then install the policy.
Creating a New AD Object

The Identity Awareness configuration wizard helps you create a new AD (Active Directory) LDAP Account Unit object in SmartDashboard. Enter the AD settings in the Integration with Active Directory window.

To create new AD Account Unit with the Identity Awareness wizard:
1. From the Integration with Active Directory window, select Create new domain.

![Integration with Active Directory window](image)

2. Enter the settings for the AD domain controller.
3. Click Connect.
   SmartDashboard connects to the AD server.
4. Click Next and then follow the instructions and finish the wizard.
   SmartDashboard creates the new AD Account Unit.

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:
- Users and user groups
- Computers and computer groups
- Networks

To create an Access Role object:
1. Select Users and Administrators in the Objects Tree.
   The Access Role window opens.
3. Enter a Name and Comment (optional) for the access role.
4. In the Networks tab, select one of these:
   - Any network
   - Specific networks - Click the plus sign and select a network.
Adding Users to the Security Policy

Your selection is shown in the Networks node in the Role Preview pane.

5. In the Users tab, select one of these:
   - Any user
   - All identified users - Includes users identified by a supported authentication method (internal users, AD users or LDAP users).
   - Specific users - Click the plus sign.
     A window opens. You can search for Active Directory entries or select them from the list.

6. In the Machines tab, select one of these:
   - Any machine
   - All identified machines - Includes computers identified by a supported authentication method (AD).
   - Specific machines - Click the plus sign.
     You can search for AD entries or select them from the list.

7. Optional: For computers that use Full Identity Agents, from the Machines tab select Enforce IP Spoofing protection.

8. Click OK.
   The access role is added to the Users and Administrators tree.

Using Identity Awareness in the Firewall Rule Base

The Identity Awareness Software Blade lets you customize the Firewall for users regardless of what computer they are using. Use Access Role objects in a rule and Identity Awareness identifies users that match the rule. You can also enable an Accept action to redirect traffic from an unidentified user to a Captive Portal.

Sample Firewall Workflow with Identity Awareness

The Firewall inspects traffic that starts from a source that matches the Access Role object. The Identity Awareness source 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.

Redirecting to a Captive Portal

You can configure rules that use an Access Role object and an Accept action, to redirect HTTP traffic to a Captive Portal. The rule allows traffic when the users for the Access Role are identified. If the Captive Portal action is enabled, these are the procedures for the Firewall to identify a user:

- The Identity Awareness source identifies the user
- 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 **Edit Properties**. The **Action Properties** window opens.
2. Select the **Redirect http connections to an authentication (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**.)

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

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.

**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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway - Retrieves LDAP user information and CRLs</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Queries LDAP user information, retrieves CRLs, and does bind operations for authentication</td>
</tr>
<tr>
<td>3</td>
<td>Security Management Server - Uses User Directory to manage user information</td>
</tr>
<tr>
<td>4</td>
<td>LDAP server - Server that holds one or more Account Units</td>
</tr>
</tbody>
</table>

Creating an Account Unit

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.

When you enable the Identity Awareness ("Creating a New AD Object" on page 53) and Mobile Access Software Blades, SmartDashboard opens a configuration wizard. The Active Directory Integration window of this wizard can create a new AD Account Unit. After you complete the wizard, SmartDashboard creates the AD object and Account Unit.
Editing an Account Unit

Use the **LDAP Account Unit Properties** window to edit an Account Unit or to create one manually.

**To open the LDAP Account Unit Properties window:**

1. In SmartDashboard, select **Manage > Servers and OPSEC Applications**. The **Servers and OPSEC Applications** window opens.
   a) To create a new Account Unit, click **New > LDAP Account Unit**.
   b) To edit an Account Unit, double-click the Account Unit object.

   The **LDAP Account Unit Properties** window opens.

2. Configure the settings in the applicable tabs.

3. Click **OK** and then click **Close**.

**General Tab**

The **General** tab lets you configure how the Security Management Server uses the Account Unit. You can select one or more of these 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. Make sure that User Directory is enabled on the Security Management Server.
- **Active Directory Query** - This AD (Active Directory) server is used as an Identity Awareness source. This option is only available if the **Profile** is set to **Microsoft_AD**.

LDAP SSO (Single Sign On) is only supported for Account Unit Objects that use **User Management**.
To configure the General tab:
1. Enter the Name for the Account Unit.
2. From Profile, select the LDAP vendor.
3. Enter the prefix or domain for the Account Unit. This value is used when the same user name is used in multiple Account Units.
   - Prefix - For servers that do NOT use AD.
   - Domain - For AD servers. This value is also necessary for AD Query and SSO.
4. Select one or more of the Account Unit usage options.
5. For LDAP user information that uses non-English languages, select Enable Unicode support.
6. To configure and enable Kerberos SSO for Identity Awareness:
   a) Click Active Directory SSO configuration.
   b) Configure the settings.
   c) Click OK.
7. Configure the other tabs or click OK.

Servers Tab
The Servers tab lets you create and manage the LDAP servers that are used by this Account Unit. You can add LDAP server objects or create new ones.

Use the Update Account to All Servers window to configure the login parameters for all the servers for this Account Unit. If the servers use different login information, edit the parameters for each server.

To configure the login parameters for all the servers:
1. Click Update Account Credentials.
   - The Update Account to All Servers window opens.
2. Enter the login parameters.
3. Click OK.

To remove a server from the Account Unit:
Select the server and click Remove.

To manage the servers for the Account Unit:
1. Do one of these actions for the server:
   - To add a server, click Add.
   - To edit a server, select the server and click Edit.
   - The LDAP Server Properties window opens.
2. If necessary, create a new SmartDashboard server object:
   a) Click New.
      - The Host Node window opens.
   b) Enter the settings for the LDAP server.
   c) Click OK.
3. From Host, select the server object.
4. Configure the settings for the LDAP server.
5. **Optional:** Click the Encryption tab and configure the SSL encryption settings.
6. Click OK.
7. Configure the other tabs or click OK.

**Objects Management Tab**

The Objects Management tab lets you select which LDAP server object SmartDashboard queries for the applicable connections and users. You can also enable password protection for this object.

To configure the Objects Management tab:
1. From Manage objects on, select the LDAP server object.
2. Click Fetch branches.
   - The Security Management Server queries and shows the LDAP branches.
3. **Optional:** Click Add, Edit and Delete to manage the LDAP branches.
4. **Optional:** Select Prompt for password when opening this Account Unit.
5. From Return entries, configure the number of entries that are stored in the LDAP database.
6. Configure the other tabs or click OK.

**Authentication Tab**

The Authentication tab lets you configure the authentication scheme for the Account Unit. You can use a common group path to optimize group membership queries. One path for all the LDAP group objects is created and only one query is necessary for the group objects.

To configure the Authentication tab:
1. **Optional:** Select Use common group path for queries.
2. Select one or more authentication schemes that are used to authenticate users in this Account Unit.
3. Select the default settings for new LDAP users:
   - **User template** - Template that you created
   - **Default authentication scheme**
4. **Optional:** Select and configure the login failure settings.
5. For IKE users in this Account Unit, enter the pre-shared secret key.
6. Configure the other tabs or click OK.

**Enabling User Directory**

Configure SmartDashboard to enable the Security Management Server to manage users in the Account Unit. You cannot use the SmartDashboard User Database when the User Directory LDAP server is enabled.

For more about using the SmartDashboard User Database, see the [R77 Security Management Administration Guide](http://supportcontent.checkpoint.com/documentation_download?ID=24830).

To enable User Directory on the Security Management Server:
   - The User Directory page opens.
2. 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) From the Network Objects tree, double-click the Security Management Server object.
   b) Click **Management** and make sure that **Network Policy Management** and **User Directory** are selected.
6. Click **OK** and 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. From the objects tree, select **Users and Administrators**.
2. Double-click the Account Unit.
   The LDAP domain is shown.
3. Double-click the LDAP branch.
   The Security Management Server queries the LDAP server and SmartDashboard shows the LDAP objects.
4. Expand the **Objects List** pane.

![Objects List Screenshot]

5. Double-click the LDAP object.
   The **Objects List** pane shows the user information.
6. Right-click a user and select **Edit**.
   The **LDAP User Properties** window opens.
7. Edit the user information and settings and then click **OK**.
Adding Users to the Rule Base

Identity Awareness and User Directory let you create rules for specified users, groups or OUs. Identity Awareness uses Access Roles that can put together users, networks gateways and other objects into a single SmartDashboard object that you can add to a rule. User Directory integrates an LDAP server and you can easily update SmartDashboard with user information.

Adding an Access Role to a Rule

Security Gateways that use the Identity Awareness Software Blade can add an Access Role as the Source or Destination of a rule. You can add SmartDashboard objects and LDAP information to the Access Role (“Working with Access Roles” on page 53) object and then use that object in the Firewall, URL Filtering, and Application Control Rule Base.

Note - Rules that use Access Role objects are enforced only on Security Gateways that have Identity Awareness enabled.

To add an Access Role to a rule:

1. From the Policy page, click the plus sign in a Source or Destination cell. The SmartDashboard window opens.

2. From the drop-down menu, select Access Roles.
3. Click the Access Role and it is added to the cell.
4. Install the policy.
Defining an Internet Access Policy

In This Section:
- Managing URL Filtering and Application Control ....................................................... 62
- HTTPS Inspection ......................................................................................................... 68

Managing URL Filtering and Application Control

Today there are many challenges for businesses to keep up with security requirements of social media and Web 2.0 applications. It is necessary for system administrators to use the security policy to overcome these challenges. For example:

- **Malware threats** - Popular applications like Twitter, Facebook, and YouTube can cause users to download viruses unintentionally. When users download files and use torrents, they can also let malware into your network.

- **Bandwidth hogging** - Applications that use a lot of bandwidth can reduce the performance for important business applications.

- **Loss of productivity** - Employees can spend time on social networking and other applications that can decrease business productivity.

- **Content control** - Prevent Internet access to websites with inappropriate content, such as sex and violence.

For more about using Application Control and URL Filtering, see the *R77 Application Control and URL Filtering Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=24853.

The Check Point Solution for Internet Browsing

The Check Point Firewall can use the URL Filtering and Application Control Software Blades to monitor and control how organizations of all sizes use the Internet. You can easily create policies which identify or block thousands of applications and Internet sites. These Software Blades help complete the security policy for your organization.

Use URL Filtering and Application Control to:

- **Create a Granular Policy** - Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels. You can also create an HTTPS policy that enables the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol.

- **Manage Bandwidth Consumption** - Configure the rules to limit the available network bandwidth for specified users or groups. You can make separate limits for uploading and downloading.

- **Keep Your Policies Updated** - The Application Database is updated regularly and makes sure that your Internet security policy has the newest applications and website categories. The Security Gateway connects to the Check Point Online Web Service to identify new social networking widgets and website categories for URLs.
• **Communicate with Users** - UserCheck objects add flexibility to URL Filtering and Application Control and let the Security Gateway communicate with users. UserCheck helps users understand that certain websites are against the company’s security policy. It also tells users about the changing Internet policy for websites and applications.

• **Create Custom Objects** - In addition to the hundreds of default objects, create new objects to manage Internet use for your network. You can create objects for applications, websites, categories and groups. Use these custom objects in rules to meet your organization’s requirements.

**UserCheck**

UserCheck works with the URL Filtering and Application Control Software Blades and lets the Security Gateway send messages to users about possible non-compliant or dangerous Internet browsing. Create rules and UserCheck objects in the URL Filtering and Application Control Rule Base to communicate with the users. These actions use UserCheck objects:

• **Inform**
• **Ask**
• **Block**

**UserCheck on a Security Gateway**

You can enable UserCheck on Security Gateways that use URL Filtering and Application Control Software Blades. When UserCheck is enabled, the user’s Internet browser shows the UserCheck messages in a new window.

**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. For example: Skype, iTunes, and Internet browser add-ons and plug-ins.
• Shows a message on the computer when it cannot be shown in the Internet browser.

**Enabling URL Filtering and Application Control**

You can enable Application Control and URL Filtering Software Blades from the **General Properties** page in SmartDashboard.

**To enable URL Filtering and Application Control:**

1. In SmartDashboard, double-click the Security Gateway. The **Gateway Properties** window opens.
2. From the navigation tree, click **General Properties**.
3. From the **Network Security** tab, select **URL Filtering, Application Control** or both.  
4. Click **OK** and install the policy.
Using the URL Filtering and Application Control Rule Base

A strong security policy uses firewall rules to inspect packets, and URL Filtering and Application Control rules to control Internet browsing. SmartDashboard has a different Rule Base that manages URL Filtering and Application Control for a Security Gateway.

These are the fields that manage the rules for the URL Filtering and Application Control security policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the URL Filtering and Application Control Rule Base.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of connections that match this rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that defines where the traffic starts.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that defines the destination of the traffic.</td>
</tr>
<tr>
<td>Applications/Sites</td>
<td>Applications or web sites that are allowed or blocked.</td>
</tr>
<tr>
<td>Action</td>
<td>Action that is done when traffic matches the rule. Options include: <strong>Allow</strong>, <strong>Block</strong>, <strong>Limit</strong> (control the bandwidth) and <strong>Inform</strong> (UserCheck message).</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the rule(s) of the policy.</td>
</tr>
<tr>
<td>Time</td>
<td>Time period that this rule is enforced.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that lets you summarize the rule.</td>
</tr>
</tbody>
</table>

Order of Rule Enforcement

The Security Gateway applies all the rules in Firewall Rule Base and then applies the URL Filtering and Application Control rules. The rules in the URL Filtering and Application Control Rule
Base are sequentially applied to packets. The first rule that matches a packet is applied. There is no Cleanup rule in the URL Filtering and Application Control Rule Base: packets that do not match the rules are allowed.

Special URL Filtering and Application Control Fields

Internet browsing is not easily defined into allowed and prohibited categories. Many websites and applications can be used for legitimate business reasons. The rules that control Internet access must be flexible and granular. The URL Filtering and Application Control Rule Base uses these fields to create a strong and flexible security policy:

- Applications/Sites
- Action

Applications/Sites

Use the Applications/Sites field to define the web applications and sites that are included in the rule. This field can use one or more of these options:

- Web applications
- Web sites
- Internet widgets
- Default categories of Internet traffic
- Custom group or category that you create

To add an application or site to a rule:

1. Click Application Control and URL Filtering > Policy.
2. Right-click the Applications/Sites cell for the rule and select one of these options:
   - Add Applications/Sites
   - Add Category

   The Application viewer window opens.
3. From the Available list, select the applications and sites for the rule.
4. Click OK.

To create a new application or site:

1. Click Application Control and URL Filtering > Applications/Sites.
2. Click New > Application/Site.
3. Select Application/Sites URLs.
4. Enter a URL and click Add.
Do this step again for all the URLs.

5. Click **Next**.

To create a custom category:

1. Click **Application Control and URL Filtering > Applications/Sites**.
2. Click **New > Application/Site Group**.
   
   The **Applications/Sites Group** window opens.
3. Enter a **Name** for the group.
4. Click **Add**.
   
   The Application viewer window opens.
5. From the **Available** list, select the applications and sites for the group.
6. Click **OK** and then click **OK**.

**Action**

Use the **Action** field to define what occurs to traffic that matches the URL Filtering and Application Control rule. These are the **Action** options:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Allows the traffic.</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks the traffic. Shows a UserCheck <strong>Block</strong> message. If no UserCheck object is defined for this action, no message is displayed.</td>
</tr>
<tr>
<td>Limit</td>
<td>Defines the maximum bandwidth that is allowed for this rule. Select or create a <strong>Limit</strong> object that defines the bandwidth limits.</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>Redirects HTTP traffic to an authentication (captive) portal. Once the user is authenticated, new connections from this source are inspected but are not redirected.</td>
</tr>
</tbody>
</table>

**Rule Actions**

- **New Rule** - Creates a new rule **Above** or **Below** the selected rule.
- **Delete Rule** - Deletes the selected rule or rules.
- **Disable Rule** - The rule stays in the Rule Base but is not active.
- **Select All Rules**
- **View rule logs in SmartView Tracker** - Opens SmartView Tracker and shows logs related to the rule.
- **View rule logs in SmartEvent** - Opens SmartEvent and shows logs related to the rule.
**UserCheck Actions**

These are the **Action** options that work with the UserCheck feature:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask</td>
<td>Shows a UserCheck <strong>Ask</strong> message. The message asks users to confirm that it is necessary that they go to the application or site.</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks the traffic. Shows a UserCheck <strong>Block</strong> message.</td>
</tr>
<tr>
<td>UserCheck Frequency</td>
<td>Defines how often users see the UserCheck message for Ask, Inform, or Block actions.</td>
</tr>
<tr>
<td>UserCheck Scope</td>
<td>Defines if the UserCheck message is shown for a category, application, or all traffic that matches the rule.</td>
</tr>
<tr>
<td>Edit UserCheck Message</td>
<td>Opens the UserCheck message in a new window.</td>
</tr>
</tbody>
</table>

**Sample URL Filtering and Application Control Rule Base**

This table shows a sample URL Filtering and Application Control Rule Base for a typical policy that monitors and controls Internet browsing. (The **Hits** and **Install On** columns are not shown.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Applications/ Sites</th>
<th>Action</th>
<th>Track</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Liability sites</td>
<td>Any</td>
<td>Internet</td>
<td>Potential liability</td>
<td>Blocked Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>High risk applications</td>
<td>Any</td>
<td>Internet</td>
<td>High Risk iTunes</td>
<td>High Risk Block</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Allow IT department Remote Admin</td>
<td>IT</td>
<td>Any</td>
<td>Radmin</td>
<td>Allow</td>
<td>Log</td>
<td>Work-Hours</td>
</tr>
<tr>
<td>4</td>
<td>Allow Facebook for HR</td>
<td>HR</td>
<td>Internet</td>
<td>Facebook</td>
<td>Allow Download_1Gbps</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>5</td>
<td>Block these categories</td>
<td>Any</td>
<td>Internet</td>
<td>Streaming Media</td>
<td>Blocked Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>6</td>
<td>Log all applications</td>
<td>Any</td>
<td>Internet</td>
<td>Any Recognized</td>
<td>Allow</td>
<td>Log</td>
<td>Any</td>
</tr>
</tbody>
</table>

1. **Liability sites** - Blocks traffic to sites and applications in the Potential_liability category. The UserCheck Blocked Message is shown to users and explains why their traffic is blocked.
2. **High risk applications** - Blocks traffic to sites and applications in the High Risk category and blocks the iTunes application. The UserCheck High Risk Block Message is shown to users and tells why their traffic is blocked.
3. **Allow IT department Remote Admin** - Allows the computers in the IT_Department network to use the Radmin application. Traffic that uses Radmin is allowed only during these hours, 8:00 - 18:30.
4. **Allow Facebook for HR** - Allows computers in the HR network to use Facebook. The total traffic downloaded from Facebook is limited to 1 Gbps, there is no upload limit.
5. **Block these categories** - Blocks traffic to these categories: Streaming Media, Social Networking, P2P File Sharing, and Remote Administration. The UserCheck Blocked Message is shown to users and explains why their traffic is blocked.

   The Remote Administration category blocks traffic that uses the Radmin application. If this rule is placed before rule 3, then this rule can also block Radmin for the IT department.

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

### 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. The Firewall cannot inspect HTTPS traffic because it is encrypted.

You can enable the HTTPS Inspection feature to let the Firewall create new SSL connections with the external site or server. The Firewall is 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 start from the Internet or an external network.

The 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 a log.

For more about configuring HTTPS Inspection, see the *R77 Application Control and URL Filtering Administration Guide* [link](http://supportcontent.checkpoint.com/documentation_download?ID=24853).

### Inspecting HTTPS Packets

#### Outbound Connections

Outbound connections are HTTPS connections that start from an internal client and connect to the Internet. The Firewall compares the HTTPS request to the HTTPS Inspection Rule Base. If the request does not match a rule, the packet is not inspected and the connection is allowed.

If the request matches an inspection rule, the Firewall makes sure that the certificate from the server (in the Internet) is valid. The Security Gateway creates a new certificate and uses it for a new HTTPS connection to the server. There are two HTTPS connections, one to the internal client and one to the server. It can then decrypt and inspect the packets according to the Firewall and other Rule Bases. The packets are encrypted again and sent to the destination.
Inbound Connections

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

If the request matches an inspection rule, the Firewall uses the certificate for the internal server to create a HTTPS connection with the external client. The Security Gateway creates a new HTTPS connection with the internal server. Since the Firewall has a secure connection with the external client, it can decrypt the HTTPS traffic. The decrypted traffic is inspected according to the Firewall and other Rule Bases.
Using the HTTPS Inspection Rule Base

The HTTPS Inspection Rule Base defines how the Firewall inspects HTTPS traffic. The HTTPS Inspection rules can use the Application Database objects 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 Rule Base is applied to all the Software Blades that have HTTPS Inspection enabled. Software Blades that can support HTTPS Inspection are:

- Application Control
- URL Filtering
- IPS
- DLP
- Anti-Virus
- Anti-Bot

HTTPS Inspection Rule Base in SmartDashboard

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the HTTPS Inspection Rule Base.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that defines where the traffic starts.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that defines the destination of the traffic.</td>
</tr>
<tr>
<td>Services</td>
<td>Type of network service that is inspected or bypassed.</td>
</tr>
<tr>
<td>Site Category</td>
<td>Categories for applications or web sites that are inspected or bypassed.</td>
</tr>
<tr>
<td>Action</td>
<td>Action that is done when HTTPS traffic matches the rule. The traffic is inspected or ignored (Bypass).</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
</tbody>
</table>
Defining an Internet Access Policy

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install On</td>
<td>Network objects that will get the HTTPS Inspection rule. You can only select Security Gateways that have HTTPS Inspection enabled.</td>
</tr>
<tr>
<td>Certificate</td>
<td>The certificate that is used for this rule.</td>
</tr>
<tr>
<td></td>
<td>• Inbound HTTPS inspection - Select the certificate that the internal server uses.</td>
</tr>
<tr>
<td></td>
<td>• Outbound HTTPS inspection - Select the Outbound Certificate object that you are using for the computers in the network.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that lets you summarize the rule.</td>
</tr>
</tbody>
</table>

Configuring Security Gateways

This section gives an example of how to configure a Security Gateway 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 policy.

Enabling HTTPS Inspection

To enable HTTPS Inspection:

1. In SmartDashboard, double-click the Security Gateway. The Gateway Properties window opens.
2. From the navigation tree, click HTTPS Inspection.
3. From Step 3, select Enable HTTP Inspection.

Generating a New Certificate

The Firewall uses a certificate to inspect outbound HTTPS traffic. You can use SmartDashboard to generate a new certificate with a password for the private key. Make sure that you export and distribute the new certificate to the endpoint computers in the network. Computers that do not have the new certificate will show SSL error messages.

To generate a new certificate for outbound HTTPS Inspection:

2. From the navigation tree, click HTTPS Inspection.
3. From Step 1, click Create certificate.
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 certificate to the endpoint computers.

### Adding a Certificate

The Firewall uses the internal server certificate to inspect inbound HTTPS traffic to the internal server. Make sure that you have a copy of the internal server certificate and the private key password before you configure inbound HTTPS inspection. The file for the certificate must have a P12 extension.

To add a server certificate for inbound HTTPS inspection:

1. Click the **Application Control and URL Filtering** tab > **Advanced**.
2. Click **HTTPS Inspection** > **Server Certificates**.
   - The **Server Certificates** page opens.
3. Click **Add**.
   - The **Import Outbound Certificate** window opens.
4. Enter the **Certificate name**.
5. Click **Browse** and select the certificate file.
6. Enter the **Private key password**.
7. Click **OK**.

### 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 ("Generating a New Certificate" on page 71). The inbound rules use a different certificate for each internal server ("Adding a Certificate" on page 72). 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.
Sample 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.)

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Site Category</th>
<th>Action</th>
<th>Blade</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Financial sites</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS</td>
<td>Financial Services</td>
<td>Bypass</td>
<td>Any</td>
<td>Outbound CA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTP_HTTPS_proxy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Outbound traffic</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS</td>
<td>Any</td>
<td>Inspect</td>
<td>Any</td>
<td>Outbound CA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTP_HTTPS_proxy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Inbound traffic</td>
<td>Any</td>
<td>WebCalendar Server</td>
<td>HTTPS</td>
<td>Any</td>
<td>Inspect</td>
<td>Any</td>
<td>WebCalendar Server CA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. **Financial sites** - Does not inspect HTTPS traffic to websites that are defined in the Financial Services category. This rule uses the Outbound CA certificate.

2. **Outbound traffic** - Inspects HTTPS traffic to the Internet. This rule uses the Outbound CA certificate.

3. **Inbound traffic** - Inspects HTTPS traffic to the network object WebCalendarServer. This rule uses the WebCalendarServer certificate.
Defending Against Network Intrusions

In This Section:

- Overview of IPS ................................................................. 74
- IPS Protection Profiles ...................................................... 74
- Enabling IPS ...................................................................... 75
- Using IPS Profiles ............................................................. 75
- Adding Network Exceptions ............................................. 76
- Browsing IPS Protections .................................................. 77
- Updating IPS Protections ................................................... 78
- Configuring Geo Protections .............................................. 78

Overview of IPS

Check Point IPS Software Blade analyzes traffic for possible risks, to enhance network security of your organization. The IPS detection engine has multiple defense layers, detects and prevents against known threats, and often protects against future ones.

For example IPS protects against drive-by downloads, where a user can go to a legitimate web site and unknowingly download malware. The malware can exploit a browser vulnerability that lets it create a special HTTP response that sends the malware to the client. The firewall allows the HTTP traffic from the web site and the computer is at risk for this malware. IPS protects the computer, it can identify and then block the drive-by download connection.

For more about using the IPS Software Blade, see the R77 IPS Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=24806.

IPS Protection Profiles

An IPS protection is a set of rules that lets you define how IPS analyzes network traffic. Create IPS profiles to easily configure one or more protections for groups of Security Gateways. You can customize the profile for the specified protections to identify specified attacks. These profiles can then be applied to the groups of Security Gateways to protect them against those attacks.

To create a new IPS protection profile:

1. In the IPS tab, select Profiles.
2. Click New and select Create New Profile.
   The General page of the Profile Properties window opens.
3. Enter the Profile Name.
4. In IPS Mode, select the default action for an IPS protection.
   - Prevent - Protections block traffic that matches the definitions.
   - Detect - Protections log traffic that matches the definitions.
5. In Protections Activation, select if protections are enabled automatically or manually.
6. From the navigation tree, click IPS Policy > Updates Policy.
7. Select the default IPS Mode for new protections that are downloaded: Prevent or Detect.
8. Click OK to create the profile.

Enabling IPS

The Enforcing Gateways page in the IPS tab shows all the Security Gateways that the IPS Software Blade is enabled. You can enable IPS on a Security Gateway that has the Firewall Software Blade enabled.

To enable IPS on a Security Gateway:

1. From the IPS tab, click Enforcing Gateways.
   The Enforcing Gateways page opens.

2. Click Add.
   The Assign Profile window opens.
3. Select a Security Gateway and click OK.
   IPS is enabled on the Security Gateway and it is shown in the Enforcing Gateways page.
4. Install the policy.

Using IPS Profiles

The Enforcing Gateways page shows all the Security Gateways that have the IPS Software Blade enabled. From this page, you can open the Gateway Properties window and assign an IPS profile to a Security Gateway.

To assign a profile to a gateway:
1. In the IPS tab, select Enforcing Gateways.
2. Select a gateway and click Edit.
The **IPS** page of the **Gateway Properties** window opens.

3. From **Assign profile**, select an IPS profile.
4. Click **OK**.

To show the Security Gateways for a profile:

1. In the **IPS** tab, select **Profiles**.
2. Select the IPS profile.
3. Click **Actions > Show Protected Gateways**.
   
   The **Protected Gateways** window opens and shows the Security Gateways that are assigned to the IPS profile.

### Adding Network Exceptions

You can configure exceptions for a protection with the **Prevent** action, so that it does not identify the specified traffic. These are some situations where it is helpful to use exceptions:

- Traffic that is legitimate for some machines or services can match the protection criteria for malware.
- A server that does not comply with RFC standards.

### Adding an IPS Exception

To add a new exception:

1. In the **IPS** tab, select **Network Exceptions**.
2. Click **New**.
   
   The **Add/Edit Exception Rule** window opens.
3. From **Profile**, select a profile or **Any**.
4. From **Protection**, select the protections to exclude.
   - **Single protection** - Click **Select** and then select the protection.
   - **All supported protections** - Only protections that support the Network Exceptions feature are excluded.
5. Define the **Source** and **Destination**, and **Service** for the excluded protection.
   - To use a SmartDashboard object, click **Manage** and then select the object.
   - To enter a value, click **IP Address** or **Port** and then enter the value.
6. Define on which Security Gateways this exception is installed. Select one of these options:
   - **All R70 gateways**
   - **Apply this exception** and select the Security Gateway object.
7. Click **OK** and then install the policy.

### Browsing IPS Protections

The **Protections** window lets you quickly see IPS protections and shows a summary of each protection.

To browse IPS protections:

Click the **IPS** tab and from the navigation tree click **Protections**.

![Protection window](image)

These columns give information about the IPS protections.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Name of the protection.</td>
</tr>
<tr>
<td>Severity</td>
<td>Probable severity of a successful attack on your environment.</td>
</tr>
<tr>
<td>Confidence Level</td>
<td>How confident IPS is that recognized attacks are actually undesirable traffic.</td>
</tr>
<tr>
<td>Performance Impact</td>
<td>How much this protection affects the performance of a Security Gateway.</td>
</tr>
<tr>
<td>Industry Reference</td>
<td>International CVE or CVE candidate name for attack.</td>
</tr>
<tr>
<td>Release Date</td>
<td>Date the protection was released by Check Point.</td>
</tr>
<tr>
<td>Follow Up</td>
<td>Shows if this protection is marked for Follow Up.</td>
</tr>
<tr>
<td>Products</td>
<td>Shows if this protection is enforced by IPS Software Blades.</td>
</tr>
<tr>
<td>Supported</td>
<td>Which Security Gateway versions support this protection.</td>
</tr>
<tr>
<td>Has an Exception</td>
<td>Shows if this protection has a network exception.</td>
</tr>
<tr>
<td>&lt;profile_name&gt;</td>
<td>There is a separate column for each IPS Profile. The cell shows the Activation setting for the protection.</td>
</tr>
</tbody>
</table>
Updating IPS Protections

Check Point is constantly developing and improving its protections against the latest threats. You can manually update the IPS protections and also set a schedule when updates are automatically downloaded and installed.

Note - The Security Gateways with IPS enabled only get the updates after you install the Policy.

To show the IPS update settings:
Click the IPS tab and from the navigation tree click Download Updates.

IPS Update Options

You can use these IPS update options to easily manage new IPS protections:

- **New protections are marked for Follow Up** - New protections can be automatically marked with a flag and are listed on the Follow Up page in the IPS tab. Click Configure to change these settings.

- **Use SmartDashboard Revision Control** - Automatically create a database revision before the IPS protections are updated. You can revert the SmartDashboard database back to the earlier IPS protections. For more information about Database Revision Control, see the R77 Security Management Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=24830.

Configuring Geo Protections

Geo Protection lets you control network traffic for specified countries. An IP-to-country database connects packet IP addresses to the countries. Configure one set of policies for each Profile to block or allow traffic for one or more countries. Configure a different policy that applies to the other countries. Private IP addresses are allowed unless the other side of 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 Protection policy.

Configure the Geo Protections for each IPS Profile separately. Policies with a Block action for Specific and Other Countries are only enabled when the Profile Action is set to Prevent.

To configure Geo Protection for specified countries:

1. Click the IPS tab and from the navigation tree click Geo Protection. The Geo Protection page opens.
2. Select the IPS Profile and one of these Geo Protection Actions for this Profile:
   - **Prevent** - The Block actions for these countries are enabled.
   - **Detect** - All traffic is allowed. Traffic that matches a policy with a Block action is logged.
   - **Inactive** - Geo Protection is disabled.
3. Optional: Click Exceptions and configure exceptions (“Adding Network Exceptions” on page 76) for the Geo Protection for this Profile.
a) Click **Country** and select the country for this policy.
b) Select the traffic **Direction** for this country.
c) From **Action**, select **Block** or **Allow**.
d) From **Track**, select a logging option.
   
   If a connection matches more than one Geo Protection policy, the first policy is logged.
e) Click **OK**.

5. Configure the Geo Protection policy for the other countries.
   a) From the drop-down menu, select **Block** or **Allow**.
   b) From **Track**, select a logging option.

6. Do these steps for all the IPS Profiles.

7. Install the policy.
   
   We recommend that after some days, you review the Geo Protection logs.
Anti-Bot and Anti-Virus

Protecting Networks from Bots

A bot is malicious software that can infect your computer. There are many infection methods, for example:

- Opening attachments that exploit a vulnerability
- Accessing 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. A botnet is a collection of compromised and infected computers.

The Anti-Bot Software Blade detects and prevents these bot and botnet threats. For more about using the Anti-Bot Software Blade, see the R77 Threat Prevention Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=24834.

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.

Check Point uses the ThreatSpect engine and ThreatCloud repository to find bots based on these procedures.

### Protecting Networks from Viruses

The Anti-Virus Software Blade inspects connections to the Internet and scans file transfers and downloads to the internal network to find and prevent malware attacks. It also gives pre-infection protection from external malware and malicious servers.

### 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 operator hideouts, 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.

### Learning about Malware

The Threat Wiki is an easy to use tool that lets you search and filter the ThreatCloud repository to find more information about identified malware. The Threat Wiki helps you to learn more about malware, you can:

- Filter by category, tag, or malware family
- Search for a malware

**To show the Threat Wiki:**

In the **Threat Prevention** tab, click **Threat Wiki**. The **Threat Wiki** page opens.
Examining Anti-Bot and Anti-Virus Protections

The **Protections** browser shows information about the Anti-Bot and Anti-Virus protections.

**To show the Protections browser:**

In the **Threat Prevention** tab, click **Protections**. The lower pane shows a detailed description of the protection type.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Name of the protection type.</td>
</tr>
<tr>
<td>Blade</td>
<td>If the protection is used by the Anti-Bot or Anti-Virus Software Blade.</td>
</tr>
<tr>
<td>Engine</td>
<td>Layer of the ThreatSpect engine that is protecting the network.</td>
</tr>
<tr>
<td>Known Today</td>
<td>Number of known protections.</td>
</tr>
<tr>
<td>&lt;Profile Name&gt;</td>
<td>For each profile, shows the action for each protection:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Prevent</strong> - Blocks traffic that matches the protection</td>
</tr>
<tr>
<td></td>
<td>• <strong>Detect</strong> - Allows all traffic and logs traffic that matches the protection</td>
</tr>
<tr>
<td></td>
<td>• <strong>Inactive</strong> - Protection is disabled</td>
</tr>
</tbody>
</table>

Protections can have more than one action. This column shows the percentage of protections set to each action.

Enabling the Anti-Bot Software Blade

Enable the Anti-Bot Software Blade on a Security Gateway.

**To enable the Anti-Bot Software Blade:**

1. In SmartDashboard, right-click the gateway object and select **Edit**.
   The **Gateway Properties** window opens.
2. In **Network Security** tab, select **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-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 the Threat Prevention policy.

Anti-Bot and Anti-Virus Rule Base

There is a different Rule Base for Anti-Bot and Anti-Virus. The Anti-Bot and Anti-Virus rules use the Malware database and network objects. Security Gateways that have Identity Awareness ("Using Identity Awareness" on page 50) 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.

The first Anti-Bot or Anti-Virus rule that matches the traffic is applied. There are no implied rules in this Rule Base, all traffic is allowed unless it is explicitly blocked. A rule that is set to the Prevent action, blocks activity and communication for that malware.

When necessary, you can add an exception directly to a rule. The object in the Protected Scope, can have a different Action from the specified Anti-Bot and Anti-Virus 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 RnD network is included in a profile with the Prevent action. You can set that network to Detect.

Managing the Anti-Bot and Anti-Virus Rule Base

These are the fields that manage the rules for the Anti-Bot and Anti-Virus threat prevention policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the Rule Base. An exception rule contains the letter E and a digit that represents the exception number. For example, E-2.2 is the second exception for the second rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Protected Scope</td>
<td>Objects that are protected against bots and viruses. Traffic to and from these objects is inspected even if the objects did not open the connection.</td>
</tr>
<tr>
<td>Protection</td>
<td>For rules, the value for this field is always N/A. The protections are set according the profile in the Action field. For exceptions, set this field to one or more specified protections.</td>
</tr>
<tr>
<td>Action</td>
<td>For rules, the value for this field is an Anti-Bot and Anti-Virus profile. For exceptions, set this field to Prevent or Detect.</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that get this rule. The default setting is All and installs the policy on all Security Gateways that have Anti-Bot and Anti-Virus enabled.</td>
</tr>
</tbody>
</table>
Sample Rule Base

This table shows a sample Anti-Bot and Anti-Virus Rule Base. (The Install On column is not shown and is set to All.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>High Security</td>
<td>Finance_server</td>
<td>- n/a</td>
<td>High_Security_Profile</td>
<td>Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corporate_internal</td>
<td></td>
<td></td>
<td>Packet Capture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corporate_finance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Malware Rule</td>
<td>Any</td>
<td>- n/a</td>
<td>Recommended_Profile</td>
<td>Log</td>
</tr>
<tr>
<td>E-2.1</td>
<td>RnD Server</td>
<td>Server_1</td>
<td>Backdoor.Win32.Shark.A</td>
<td>Detect</td>
<td>Log</td>
</tr>
</tbody>
</table>

1. **High Security** - Traffic for the Finance server and two corporate networks are inspected for bots and viruses according to the settings in the High_Security profile. The traffic is logged and the packets are captured for analysis in SmartView Tracker.

2. **Malware Rule** - All traffic in the network is inspected for bots and viruses according to the settings in the Recommend_Profile.

E-2.1 **RnD Server** - A global exception rule for the Server-1 object, that only detects the Backdoor.Win32.Shark.A protection.

E-2.2 **Users_3** - An exception rule for the Users_3 Access Role, that only detects some protections.

**Anti-Spam**

Employees waste more and more time to sort through bulk emails commonly known as spam. The amount of resources (disk space, network bandwidth, CPU) devoted to handling spam also increases from year to year. In addition, unwanted emails continue to grow and can be an unexpected security threat to networks. Cyber-criminals can use emails to let viruses and malware into your network. The Anti-Spam and Mail Software Blade gives system administrators an easy and central tool to eliminate most of the spam that reaches their networks.

**Enabling Anti-Spam**

Use the **Overview** page in the **Anti-Spam & Mail** tab to enable Anti-Spam on a Security Gateway.

**To enable Anti-Spam:**

1. In the **Anti-Spam & Mail** tab, select **Overview**.
2. Click **Anti-Spam**.
   - The **Anti-Spam Enforcing Gateways** window opens.
3. Select one or more Security Gateways.
4. Click **OK**.
## Sample Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content based Anti-Spam</td>
<td>High protection</td>
<td>Identifies spam based on email content</td>
</tr>
<tr>
<td>IP Reputation Anti-Spam</td>
<td>High protection</td>
<td>Identifies spam based on IP address database of known spammers</td>
</tr>
<tr>
<td>Block List Anti-Spam</td>
<td>Block</td>
<td>Identifies spam based on domains or IP addresses that you define</td>
</tr>
<tr>
<td>Mail Anti-Virus</td>
<td>Block</td>
<td>Scans and filters emails for viruses and other malware</td>
</tr>
<tr>
<td>Zero hour malware protection</td>
<td>Off</td>
<td>Does not scan the Internet to identify and filter new virus email attacks</td>
</tr>
</tbody>
</table>

The **Zero hour malware protection** feature is set to **Off** because enabling the feature has a negative effect on network performance.
Securing Data

In This Section:

Overview ........................................................................................................................ 86
Enabling DLP ................................................................................................................ 89
DLP Rule Base .............................................................................................................. 91
Analyzing and Tracking DLP ........................................................................................ 94

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" on page 63).

• **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.

Sample DLP Deployment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway configured with DLP</td>
</tr>
<tr>
<td>3</td>
<td>Web server in the DMZ</td>
</tr>
<tr>
<td>4</td>
<td>Mail relay in the DMZ</td>
</tr>
<tr>
<td>5</td>
<td>Internal computers</td>
</tr>
<tr>
<td>6</td>
<td>AD or LDAP server</td>
</tr>
<tr>
<td>7</td>
<td>Internal Exchange server with Exchange Security Agent</td>
</tr>
<tr>
<td>8</td>
<td>SmartEvent and SmartView Tracker server</td>
</tr>
<tr>
<td>9</td>
<td>SmartConsoles and Security Management Server</td>
</tr>
</tbody>
</table>

2. The Security Gateway uses the built-in data types and rules to supply out-of-the-box Data Loss Prevention. DLP can also use the AD or LDAP server to identify users in the internal organization.
3. The Security Gateway analyzes all traffic from the web and mail server before it goes to the Internet. It catches all traffic containing data and being sent through supported protocols. It scans the traffic, including email attachments, for data that should be protected from being sent to external networks. This data is recognized by protocol, source, destination, and complex data type representations.
The Security Gateway can also inspect internal traffic between Microsoft Exchange clients in the organization. The Exchange Security Agent forwards internal emails to DLP.

4. SmartView Tracker and SmartEvent log, track, analyze events, and report incidents that are captured by DLP.

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 R77 DLP Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=24852.

Sample Mail Relay Deployment

In this deployment the Security Gateway with the DLP Software Blade scans emails once, as they are sent from an internal mail server (such as Microsoft Exchange) to a mail relay in the DMZ. The Security Gateway scans the email before it reaches the mail relay. The mail relay can send the allowed emails to internal and external recipients.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway configured with DLP</td>
</tr>
<tr>
<td>3</td>
<td>Mail relay in the DMZ</td>
</tr>
<tr>
<td>4</td>
<td>Internal mail server</td>
</tr>
<tr>
<td>5</td>
<td>Internal computers</td>
</tr>
</tbody>
</table>
Mail Relay Workflow
1. User at internal computer sends email.
2. Email reaches the internal mail server and is forwarded to the mail relay.
3. Security Gateway intercepts and scans the email.
   - Email matches a Prevent rule - email is not forwarded
   - Email matches an Ask User rule - User must confirm that the email does not violate the DLP policy to forward it
   - Email matches Inform User, Detect, or no rule - email is forwarded
4. The mail relay receives the email from the Security Gateway and sends it to the internal or external recipient.

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. From the Network Objects tree, double-click the Security Gateway.
   The General Properties window opens.
2. In the Network Security tab, select Data Loss Prevention.
   The Data Loss Prevention Wizard opens.
3. Click Next.
   The Email Domain and Active Directory page opens.
4. Enter the email domain for your company to let DLP distinguish between internal and external email addresses.
5. 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.
6. Click Next.
   The My Organization Name page opens.
7. Enter different names and phrases that are used to identify your organization.
   DLP uses these names to accurately detect incidents of data loss.
8. Click Next.
   The DLP Portal and Mail Server page opens.
   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.
10. **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**.

11. Click **Next**. The **Protocols** page opens.

12. Select one or more of these protocols to which the DLP policy applies.
   - Email
   - Web
   - File Transfer

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

14. 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 the **Data Loss Prevention** tab, select **Data Types**.
2. Double-click a data type. The Data Type properties window opens.
3. From the navigation tree, select **Data Owners**.
4. Click **Add**. The **Add Data Owners** window opens.
5. 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).
6. Add as many data owners as needed.
7. 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 the **Data Loss Prevention** tab, select **Policy**.
2. Right-click the **Track** cell of the rule and select **Email**. The **Email** window opens.
3. Select **When data is matched**. **Data Owners** are added to the Email Notification list.
4. **Optional:** Click **Add** to send notification emails to more users.
5. 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

6. 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 SmartDashboard and on the Exchange server. For more about configuring an Exchange Security Agent, see the R77 DLP Administration Guide [http://supportcontent.checkpoint.com/documentation_download?ID=24852](http://supportcontent.checkpoint.com/documentation_download?ID=24852).

**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 easily create and configure DLP rules.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flag</td>
<td>Mark a rule to <strong>Follow Up</strong> or <strong>Improve Accuracy</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the rule.</td>
</tr>
<tr>
<td>Data</td>
<td>Data type for this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Who or what starts the connection: Users and Administrators, network, or email domains. If Identity Awareness is enabled, you can use Access Roles.</td>
</tr>
</tbody>
</table>
### Field Description

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

### DLP Rule Exceptions

When a data transmission matches the exception of a DLP rule, the data is bypasses the rule, and 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 the **Data Loss Prevention** tab, select **Policy**.
   
   The **Policy** window opens and shows the DLP Rule Base.
2. Right-click the **Exceptions** cell for a rule and select **Edit**.
   
   The **Exceptions for Rule** window opens.
3. Click **New Exception**.
4. Configure these settings for the exception: **Data Type**, **Source**, **Destination**, **Protocol**.
5. Click **OK** and then 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect</td>
<td>The Firewall sends the data. The event is logged in SmartView Tracker and is available for your review and analysis in SmartReporter and SmartEvent. The data and the email itself, or the properties of the transmission if not email, are saved in storage for future reference.</td>
</tr>
<tr>
<td>Inform User</td>
<td>The Firewall sends the data, but the incident is logged and the user is notified.</td>
</tr>
</tbody>
</table>
### Action | Description
--- | ---
**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 SmartView Tracker under the User Actions category. Administrators with full permissions or with the View/Release/Discard DLP messages permission can also decide whether the transmission should be completed or not from SmartView Tracker. This can be useful in the event that a user is not available to make sure if it should be sent.

**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

<table>
<thead>
<tr>
<th>Flag</th>
<th>Name</th>
<th>Data</th>
<th>Exceptions</th>
<th>Action</th>
<th>Track</th>
<th>Severity</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Follow Up</td>
<td>Salesforce Reports</td>
<td>Salesforce Reports</td>
<td>None</td>
<td>Ask User</td>
<td>Log</td>
<td>High</td>
<td>Business</td>
</tr>
<tr>
<td>No Flag</td>
<td>PCI - Credit Card Numbers</td>
<td>PCI - Cardholder Data</td>
<td>None</td>
<td>Prevent</td>
<td>Log</td>
<td>Critical</td>
<td>Compliance</td>
</tr>
<tr>
<td>No Flag</td>
<td>SEC Filings - Draft or Recent</td>
<td>SEC Filings - Draft or Recent</td>
<td>None</td>
<td>Detect</td>
<td>Log</td>
<td>High</td>
<td>Financial</td>
</tr>
<tr>
<td>No Flag</td>
<td>Source Code</td>
<td>Source Code</td>
<td>1</td>
<td>Detect</td>
<td>Alert</td>
<td>High</td>
<td>Intellectual Property</td>
</tr>
</tbody>
</table>

**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 SmartConsole clients can help with your DLP analysis:

• SmartView Tracker
• 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 SmartView Tracker or SmartEvent, Microsoft Office 2010 must be installed. These SmartConsole clients do not show DLP incidents, if these EML files are associated with another application.

Using SmartView Tracker

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 use SmartView Tracker to analyze DLP:
1. In SmartDashboard, select SmartConsole > SmartView Tracker.
2. In the Network & Endpoint tab, select Predefined > Data Loss Prevention Blade.
3. Double-click a category.
   The Data Loss Prevention logs for the category are shown.

DLP Actions

SmartView Tracker actions for DLP incidents include:

<table>
<thead>
<tr>
<th>DLP Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask User</td>
<td>DLP incident captured and put in Quarantine, user asked to decide what to do</td>
</tr>
<tr>
<td>DLP Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Do not Send</td>
<td>User decided to drop transmission that was captured by DLP. An administrator with full permissions or with the View/Release/Discard DLP messages permission can also drop these transmissions. Email notification is sent to the user.</td>
</tr>
<tr>
<td>Send</td>
<td>User decided to continue transmission after DLP capture. An administrator with full permissions or with the View/Release/Discard DLP messages permission can also decide to continue transmission. Email notification is sent to the user.</td>
</tr>
<tr>
<td>Quarantine Expired</td>
<td>DLP captured data transmission cannot be sent because the user did not make a decision in time. Expired incidents may still be viewed, until they are deleted (routine cleanup process).</td>
</tr>
<tr>
<td>Prevent</td>
<td>DLP transmission was blocked.</td>
</tr>
<tr>
<td>Allow</td>
<td>DLP transmission was allowed; usually by exception to rule.</td>
</tr>
<tr>
<td>Inform User</td>
<td>DLP transmission was detected and allowed, and user notified.</td>
</tr>
<tr>
<td>Deleted Due To Quota</td>
<td>DLP incidents are deleted from gateway for disk space.</td>
</tr>
</tbody>
</table>

**DLP General Columns**

DLP incidents can show some or all of these columns and are available to all administrators.

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

**Using the Incident UID as a key between multiple logs:**

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

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

Each matched Data Type generates its own log. The gateway makes sure that all the Data Type logs of one incident show the same unique Incident UID and rule action (Prevent, Ask, Inform, or Detect). This happens also if Data Types were matched on different rules. The same action shown for an incident is the most restrictive.
For example, in a case that a transmission matches two Data Types. Each Data Type is used in a different rule. The action of one rule is Prevent. The action in the second rule is Detect. The two logs that are generated will show Prevent as the action. The action implemented will be Prevent. The log of the Detect rule will show *Rule Base (Action set by different rule)* in the **DLP Action Reason** column.

**DLP Restricted Columns**

These columns are restricted to administrators with permissions.

<table>
<thead>
<tr>
<th>Restricted Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UserCheck</strong></td>
<td></td>
</tr>
<tr>
<td>User Response</td>
<td>Comment entered by the user in the text box shown in the UserCheck notification.</td>
</tr>
<tr>
<td>UserCheck Message to User</td>
<td>The message shown to the user.</td>
</tr>
<tr>
<td>Interaction Name</td>
<td>The interaction name as shown in SmartDashboard.</td>
</tr>
<tr>
<td><strong>Fingerprint</strong></td>
<td></td>
</tr>
<tr>
<td>Matched File</td>
<td>The file name and path in the scanned fingerprint repository that matches the inspected message.</td>
</tr>
<tr>
<td>Matched File Percentage</td>
<td>How much is this file similar to Matched File. In “exact match” this will always be 100%.</td>
</tr>
<tr>
<td>Matched File Text Segments</td>
<td>In a partial match, the number of file parts/segments that are matched between the Matched File and the inspected file (parts/segment may overlap).</td>
</tr>
<tr>
<td><strong>DLP Type</strong></td>
<td></td>
</tr>
<tr>
<td>DLP Rule Name</td>
<td>Name of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>Message to User</td>
<td>Message sent, as configured by administrator, for the rule on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Words List</td>
<td>If the Data Type on which the incident was matched included a word list (keywords, dictionary, and so on), the list of matched words.</td>
</tr>
<tr>
<td>DLP Relevant Data Types</td>
<td>If matched Data Type is a group Data Type. This field specifies which Data Types from that group were matched.</td>
</tr>
<tr>
<td><strong>User Information</strong></td>
<td></td>
</tr>
<tr>
<td>DLP Recipients</td>
<td>For SMTP traffic, list of recipients of captured email.</td>
</tr>
<tr>
<td>Mail Subject</td>
<td>For SMTP traffic, the subject of captured email.</td>
</tr>
</tbody>
</table>
### Restricted Filters

<table>
<thead>
<tr>
<th>Description</th>
<th>Scanned Data Fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captured data itself: email and attachment of SMTP, file of FTP, or HTTP traffic.</td>
<td></td>
</tr>
</tbody>
</table>

### More

<table>
<thead>
<tr>
<th>Description</th>
<th>UserCheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>A boolean field that shows if the log is produced by UserCheck or by another DLP.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Data Type Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the matched Data Type.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Data Type UID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal ID of the Data Type on which the incident was matched.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>DLP Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category of Data Type on which the incident was matched.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>DLP Template Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>A measurement, expressed as a percentage, that shows how closely a document matches the template file.</td>
<td></td>
</tr>
<tr>
<td>0% - The document and template are very different.</td>
<td></td>
</tr>
<tr>
<td>100% - The document and template are a close match.</td>
<td></td>
</tr>
</tbody>
</table>

### Using SmartEvent

SmartEvent provides advanced analysis tools with filtering, charts, reporting, statistics, and more, of all events that pass through enabled Security Gateways. SmartEvent combines all DLP logs of the same incident (all matching rules and Data Types and user action if applicable) to a single event.

You can filter out the specific Data Loss Prevention information for efficient monitoring and relevant reporting on DLP incidents.

- Real-time and history graphs and reports of Data Loss Prevention incidents
- Graphical incident timelines for rapid information retrieval
- Easily configured custom views to quickly answer specific queries
- Incident management workflow
- Reports to data owners on a scheduled basis

**To open SmartEvent:**

1. In SmartDashboard, select **Window > SmartEvent**.
2. When SmartEvent is open, open **Events**.
3. Select **Predefined > DLP** or any of the analysis data categories under **DLP**.
Maximizing Network Performance

In This Section:

Check Point Software Acceleration Solutions ............................................................ 98
CoreXL ........................................................................................................................... 98
Using SecureXL............................................................................................................. 99
Multi-Queue ................................................................................................................ 100

Check Point Software Acceleration Solutions

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

- CoreXL
- SecureXL (Performance Pack)

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. You cannot configure CoreXL and SecureXL with SmartDashboard, instead run the applicable commands from the CLI.

For more about configuring CoreXL and SecureXL, see the R77 Performance Tuning Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=24808.

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.

<table>
<thead>
<tr>
<th>Number of Cores</th>
<th>Number of Kernel Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>6-20</td>
<td>Number of cores, minus 2</td>
</tr>
<tr>
<td>More than 20</td>
<td>Number of cores, minus 4 -- but no more than 30</td>
</tr>
</tbody>
</table>
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.

Using 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 and you cannot use SmartDashboard to configure it.

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

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
<table>
<thead>
<tr>
<th>Multi-Queue disabled</th>
<th>CPU cores for SND</th>
<th>CPU cores for CoreXL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Multi-Queue enabled</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>
Configuring the NAT Policy

Translating IP Addresses

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 SmartDashboard 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.

SmartDashboard 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.
- SmartDashboard 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 ("Automatic and Manual NAT Rules" on page 105) to use Port Translation.
Using Hide NAT

For each SmartDashboard object, you can configure the IP address that is used to translate addresses for Hide NAT mode:

- Use the IP address of the external Security Gateway interface
- Enter an IP address for the object

Hide NAT uses dynamically assigned port numbers to identify the original IP addresses. There are two pools of port numbers: 600 to 1023, and 10,000 to 60,000. Port numbers are usually assigned from the second pool. The first pool is used for these services:

- rlogin [destination port 512]
- rshell [destination port 513]
- rexec [destination port 514]

If the connection uses one of these services, and the source port number is below 1024, then a port number is assigned from the first pool.

You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

Sample NAT Deployments

**Static NAT**

Firewalls that do Static NAT, translate each internal IP address to a different external IP address.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Firewall is configured with Static NAT</td>
</tr>
<tr>
<td>3</td>
<td>Internal computers</td>
</tr>
</tbody>
</table>
Sample Static NAT Workflow

An external computer in the Internet sends a packet to 192.0.2.5. The Firewall translates the IP address to 10.10.0.26 and sends the packet to internal computer A. Internal computer A sends back a packet to the external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.5.

Internal computer B (10.10.0.37) sends a packet to an external computer. The Firewall intercepts the packet translates the source IP address to 192.0.2.16.

Hide NAT

Firewalls that do Hide NAT use different port numbers to translate internal IP address to one external IP address. External computers cannot start a connection to an internal computer.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Firewall is configured with Hide NAT</td>
</tr>
<tr>
<td>3</td>
<td>Internal computers</td>
</tr>
</tbody>
</table>
Sample Hide NAT Workflow

Internal computer A (10.10.0.26) sends a packet to an external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.1 port 11000. The external computer sends back a packet to 192.0.2.1 port 11000. The Firewall translates the packet to 10.10.0.26 and sends it to internal computer A.

NAT Rule Base

The NAT Rule Base has two sections that specify how the IP addresses are translated:

- **Original Packet**
- **Translated Packet**

Each section in the NAT Rule Base is divided into cells that define the **Source**, **Destination**, and **Service** for the traffic.

Automatic and Manual NAT Rules

There are two types of NAT rules for network objects:

- Rules that SmartDashboard automatically creates and adds to the NAT Rule Base
- Rules that you manually create and then add to the NAT Rule Base

When you create manual NAT rules, it can be necessary to create the translated NAT objects for the rule.

Using Automatic Rules

You can enable automatic NAT rules for these SmartDashboard objects:

- Security Gateways
- Nodes
- Networks
- Address Ranges

SmartDashboard creates two automatic rules for Static NAT to translate both the source and destination of the packets. One rule is created for Hide NAT to translate the source of the packets.

For network and address range objects, SmartDashboard creates a different rule to NOT translate intranet traffic. IP addresses for computers on the same object are not translated.
This table summarizes the NAT automatic rules:

<table>
<thead>
<tr>
<th>Type of Traffic</th>
<th>Static NAT</th>
<th>Hide NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal to external</td>
<td>Rule translates source IP address</td>
<td>Rule translates source IP address</td>
</tr>
<tr>
<td>External to internal</td>
<td>Rule translates destination IP address</td>
<td>N/A (External connections are not allowed)</td>
</tr>
<tr>
<td>Intranet (for network and address range objects)</td>
<td>Rule does not translate IP address</td>
<td>Rule does not translate IP address</td>
</tr>
</tbody>
</table>

Order of NAT Rule Enforcement

The Firewall enforces the NAT Rule Base in a sequential manner. Automatic and manual rules are enforced differently. Automatic rules can use bidirectional NAT to let two rules be enforced for a connection.

- **Manual rules** - The first manual NAT rule that matches a connection is enforced. The Firewall does not enforce a different NAT rule that can be more applicable.
- **Automatic rules** - Two automatic NAT rules that match a connection, one rule for the **Source** and one for the **Destination** can be enforced. When a connection matches two automatic rules, those rules are enforced.

SmartDashboard organizes the automatic NAT rules in this order:
1. Static NAT rules for Firewall, or node (computer or server) objects
2. Hide NAT rules for Firewall, or node objects
3. Static NAT rules for network or address range objects
4. Hide NAT rules for network or address range objects

Sample Automatic Rules

**Static NAT for a Network Object**

1. Intranet connections in the HR network are not translated. The Firewall does not translate a connection between two computers that are part of the HR object. The Firewall does not apply rules 2 and 3 to traffic that matches rule 1.
2. Connections from IP addresses from the HR network to any IP address (usually external computers) are translated to the Static NAT IP address.
3. Connections from any IP address (usually external computers) to the HR are translated to the Static NAT IP address.
**Hide NAT for Address Range**

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Packet</th>
<th>Translated Packet</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source</td>
<td>Destination</td>
<td>Service</td>
</tr>
<tr>
<td>1</td>
<td>Sales</td>
<td>Sales</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>Sales</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

1. Intranet connections in the Sales address range are not translated. The Firewall does not translate a connection between two computers that use IP addresses that are included in the Sales object.
   The Firewall does not apply rule 2 to traffic that matches rule 1.
2. Connections from IP addresses from the Sales address range to any IP address (usually external computers) are translated to the Hide NAT IP address.

**Configuring Static and Hide NAT**

Use the **NAT** page in the **Gateway Properties** window to enable and configure NAT for SmartDashboard objects.

**Configuring Static NAT**

When you enable Static NAT, each object is translated to a different IP address. SmartDashboard can automatically create the NAT rules, or you can create them manually.

**Configuring Hide NAT**

Hide NAT uses different port numbers to identify the internal IP addresses. When you enable Hide NAT mode, the Firewall can translates the IP address to:

- The IP address of the external Security Gateway interface
- The IP address for the object

**Note** - You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

**Enabling Automatic NAT**

SmartDashboard can automatically create and configure the NAT rules for a network. Enable automatic NAT for each object that you are translating the IP address. Then configure the Firewall Rule Base to allow traffic to the applicable objects.

**To enable automatic NAT:**

1. Double-click the SmartDashboard object.
   The **General Properties** window opens.
2. Click **NAT**.
3. Select **Add Automatic Address Translation rules**.
4. Select the **Translation method**: **Hide** or **Static**.
5. Configure the NATed IP address for the object.
   - **Hide behind Gateway** - Use the Security Gateway IP address.
   - **Hide behind IP address** - Enter the IP address.
6. Click **Install on Gateway** and select **All** or the Security Gateway that translates the IP address.
7. Click **OK**.
8. Do these steps for all the applicable objects.
9. Click **Firewall > Policy**.
   The **Policy** page opens and shows the Firewall Rule Base.
10. Add rules that allow traffic to the applicable objects.
11. Install the policy.

### Automatic Hide NAT to External Networks

For large and complex networks, it can be impractical to configure the Hide NAT settings for all the internal IP addresses. An easy alternative is to enable a Firewall to automatically Hide NAT for all traffic with external networks. The Firewall translates all traffic that goes through an external interface to the valid IP address of that interface.

In this sample configuration, computers in internal networks open connections to external servers on the Internet. The source IP addresses of internal clients are translated to the IP address of the external interface.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Firewall is configured with automatic Hide NAT. There are two external interfaces <strong>192.0.2.1</strong> and <strong>192.0.2.100</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Internal computers</td>
</tr>
</tbody>
</table>

The source IP address is translated to the applicable external interface IP address: **192.0.2.1** or **192.0.2.100**.

**Note** - If a connection matches a regular NAT rule and a NAT-for-internal-networks rule, the regular NAT rule takes precedence.
To enable automatic Hide NAT:
1. Double-click the Security Gateway.
   The **Gateway Properties** window opens.
2. From the navigation tree, click **NAT**.
   The **NAT** page opens.
3. Select **Hide internal networks behind the Gateway external IP**.
4. Click **OK** and then install the policy.

**Enabling Manual NAT**

For some deployments, it is necessary to manually define the NAT rules. Create SmartDashboard objects that use the **valid** (NATed) IP addresses. Create NAT rules to translate the original IP addresses of the objects to valid IP addresses. Then configure the Firewall Rule Base to allow traffic to the applicable translated objects with these valid IP addresses.

**Note** - For manual NAT rules, it is necessary to configure proxy ARPs to associate the translated IP address ("Automatic and Proxy ARP" on page 113).

These are some situations that must use manual NAT rules:
- Rules that are restricted to specified destination IP addresses and to specified source IP addresses
- Translate both source and destination IP addresses in the same packet.
- Static NAT in only one direction
- Translate services (destination ports)
- Rules that only use specified services (ports)
- Translate IP addresses for dynamic objects

This procedure explains how to configure manual Static NAT for a web server. You can also configure manual Hide NAT for SmartDashboard objects ("Sample Deployment (Manual Rules for Port Translation)" on page 111).

To enable manual Static NAT:
1. Right-click the object in SmartDashboard and select **Clone**.
   The **General Properties** window of the new object opens.
2. Enter the **Name**. We recommend that you name the object `<name>_valid_address`.
3. Enter the NATed IP address.
4. Click **OK**.
5. Click **Firewall > NAT**.
   The **NAT** page opens and shows the NAT Rule Base.
6. Add a manual rule above the automatic NAT rules.
7. Configure the manual rule to translate the IP address. For example:
   - Original Packet Source - **WebServer**
   - Translated Packet Source - **WebServer_valid_address**
8. Click **Firewall > Policy**.
   The **Policy** page opens and shows the Firewall Rule Base.
9. Add rules that allow traffic to the applicable NATed objects. These objects are the cloned objects that are called `<name>_valid_address`.

10. Install the policy.

Sample Deployment (Static and Hide NAT)

The goal for this sample deployment is to configure:

- Static NAT for the SMTP and the HTTP servers on the internal network. These servers can be accessed from the Internet using public addresses.
- Hide NAT for the users on the internal network that gives them Internet access. This network cannot be accessed from the Internet.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway (External interface 2001:db8:0:a::1)</td>
</tr>
<tr>
<td>3</td>
<td>Internal computers (Alaska_LAN 2001:db8::/64)</td>
</tr>
<tr>
<td>4</td>
<td>Web server (Alaska.Web 2001:db8:0:10::5 translated to 2001:db8:0:a::5)</td>
</tr>
<tr>
<td>5</td>
<td>Mail server (Alaska.Mail 2001:db8:0:10::6 translated to 2001:db8:0:a::6)</td>
</tr>
</tbody>
</table>

To configure NAT for the network:

1. Enable automatic Static NAT for the web server.
   a) Double-click the Alaska.Web object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Static**.
   d) Select **Hide behind IP Address** and enter 2001:db8:0:a::5.
   e) Click **OK**.
2. Enable automatic Static NAT for the mail server.
   a) Double-click the Alaska.Mail object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Static**.
   d) Select **Hide behind IP Address** and enter 2001:db8:0:a::6.
   e) Click **OK**.

3. Enable automatic Hide NAT for the internal computers.
   a) Double-click the Alaska_LAN object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Hide**.
   d) Select **Hide behind Gateway**.

4. Click **OK** and then install the policy.

**Sample Deployment (Manual Rules for Port Translation)**

The goal for this sample configuration is to let external computers access a web and mail server in a DMZ network from one IP address. Configure Hide NAT for the DMZ network object and create manual NAT rules for the servers.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway (Alaska_GW external interface 2001:db8:0:c::1)</td>
</tr>
<tr>
<td>3</td>
<td>DMZ network (Alaska_DMZ 2001:db8:a::/128)</td>
</tr>
<tr>
<td>4</td>
<td>Web server (Alaska_DMZ_Web 2001:db8:a::35:5 translated to 2001:db8:0:c::1)</td>
</tr>
<tr>
<td>5</td>
<td>Mail server (Alaska_DMZ_Mail 2001:db8:a::35:6 translated to 2001:db8:0:c::1)</td>
</tr>
</tbody>
</table>
To configure NAT for the DMZ servers:

1. Enable automatic Hide NAT for the DMZ network.
   a) Double-click the Alaska_DMZ object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Hide**.
   d) Select **Hide behind Gateway**.
   e) Click **OK**.

2. Create a manual NAT rule that translates HTTP traffic from the Security Gateway to the web server.
   a) In the **Firewall** tab, select **NAT**.
   b) Add a rule below the automatic rules.
   c) Right-click the cell and select **Add Object** to configure these settings:
      - **Original Destination** - Alaska_GW
      - **Original Service** - HTTP
      - **Translated Destination** - Alaska_DMZ_Web

3. Create a manual NAT rule that translates SMTP traffic from the Security Gateway to the mail server.
   a) Add a rule below the automatic rules.
   b) Right-click the cell and select **Add Object** to configure these settings:
      - **Original Destination** - Alaska_GW
      - **Original Service** - SMTP
      - **Translated Destination** - Alaska_DMZ_Web

4. Create a rule in the Firewall Rule Base that allows traffic to the servers.
   a) In the **Firewall** tab, select **Policy**.
   b) Add a rule to the Rule Base.
   c) Right-click the cell and select **Add Object** to configure these settings:
      - **Destination** - Alaska_DMZ
      - **Service** - HTTP, SMTP
      - **Action** - Allow

5. Install the policy.

### NAT Rule Base for Manual Rules for Port Translation Sample Deployment

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Original Packet</th>
<th>Service</th>
<th>Source</th>
<th>Translated Packet</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Original</td>
<td>All</td>
<td>Automatic rule</td>
</tr>
<tr>
<td>2</td>
<td>Alaska_DMZ</td>
<td>Alaska_DMZ</td>
<td>Any</td>
<td>Alaska_DMZ</td>
<td>Original</td>
<td>All</td>
<td>Automatic rule</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Alaska,GW</td>
<td>http</td>
<td>Original</td>
<td>Alaska_DMZ_Vi</td>
<td>Policy Targets</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Alaska,GW</td>
<td>smtp</td>
<td>Original</td>
<td>Alaska_DMZ_M</td>
<td>Policy Targets</td>
<td></td>
</tr>
</tbody>
</table>
Advanced NAT Settings

Deployment Configurations

This section discusses how to configure NAT in some network deployments.

**Automatic and Proxy ARP**

Giving a machine in the internal network an external IP address using NAT makes that machine appear to the Internet to be on the external network, or the Internet side of the firewall. When NAT is configured automatically, the Security Gateway replies on behalf of translated network objects to ARP requests from the Internet router for the address of the internal machine.

If you are using manual rules, you must configure proxy ARPs to associate the translated IP address with the MAC address of the Security Gateway interface that is on the same network as the translated addresses.

For more about configuring Proxy ARP for IPv4 Manual NAT, see sk30197 [http://supportcontent.checkpoint.com/solutions?id=sk30197].

For more about configuring Proxy NDP for IPv6 Manual NAT, see sk91905 [http://supportcontent.checkpoint.com/solutions?id=sk91905].

**NAT and Anti-Spoofing**

NAT is performed after Anti-Spoofing checks, which are performed only on the source IP address of the packet. This means that spoofing protection is configured on the interfaces of the Security Gateway in the same way as NAT.
Disabling NAT in a VPN Tunnel

When communicating within a VPN, it is normally not necessary to perform NAT. You can disable NAT in a VPN tunnel with a single click in the VPN community object. Disabling NAT in a VPN tunnel by defining a NAT rule slows down the performance of the VPN.

Connecting Translated Objects on Different Interfaces

The following sections describe how to allow connections in both directions between statically translated objects (nodes, networks or address ranges) on different Security Gateway interfaces.

If NAT is defined through the network object (as opposed to using Manual NAT Rules), then you must ensure that bidirectional NAT is enabled.

Internal Communication with Overlapping Addresses

If two internal networks have overlapping (or partially overlapping) IP addresses, Security Gateway enables:

- Communication between the overlapping internal networks.
- Communication between the overlapping internal networks and the outside world.
- Enforcement of a different security policy for each overlapping internal network.

Network Configuration

For example, assume both Network A and Network B share the same address space (192.168.1.0/24), therefore standard NAT cannot be used to enable communication between the two networks. Instead, overlapping NAT must be performed on a per interface basis.
Users in Network A who want to communicate with users in Network B must use the 192.168.30.0/24 network as a destination. Users in Network B who want to communicate with users in Network A must use the 192.168.20.0/24 network as a destination.

The Security Gateway translates the IP addresses in the following way for each individual interface:

**Interface A**
- Inbound source IP addresses are translated to the virtual network 192.168.20.0/24.
- Outbound destination IP addresses are translated to the network 192.168.1.0/24.

**Interface B**
- Inbound source IP addresses are translated to the network 192.168.30.0/24.
- Outbound destination IP addresses are translated to the network 192.168.1.0/24.

**Interface C**
Overlapping NAT is not configured for this interface. Instead, use NAT Hide in the normal way (not on a per-interface basis) to hide source addresses behind the interface’s IP address (192.168.4.1).

**Communication Examples**
This section describes how to enable communication between internal networks, and between an internal network and the Internet.

**Communication Between Internal Networks**
If user A, at IP address 192.168.1.10 in Network A, wants to connect to user B, at IP address 192.168.1.10 (the same IP address) in Network B, user A opens a connection to the IP address 192.168.30.10.

**Communication Between an Internal Network and the Internet**
If user A, at IP address 192.168.1.10 in network A, connects to IP address 10.10.10.10 on the Internet.
Communication Between an Internal Network and the Internet

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface A — before NAT</td>
<td>192.168.1.10</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Interface A — after NAT</td>
<td>192.168.20.10</td>
<td>10.10.10.10</td>
</tr>
</tbody>
</table>

Security Gateway enforces the security policy for packets from network **192.168.20.0/24** to the Internet.

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface C — before NAT</td>
<td>192.168.20.10</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Interface C — after NAT Hide</td>
<td>192.168.4.1</td>
<td>10.10.10.10</td>
</tr>
</tbody>
</table>

Routing Considerations
To allow routing from Network A to Network B, routing must be configured on the Firewall.

These sections contain sample routing commands for Windows and Linux operating systems (for other operating systems, use the equivalent commands).

**On Windows**
- `route add 192.168.30.0 mask 255.255.255.0 192.168.3.2`
- `route add 192.168.20.0 mask 255.255.255.0 192.168.2.2`

**On Linux**
- `route add -net 192.168.30.0/24 gw 192.168.3.2`
- `route add -net 192.168.20.0/24 gw 192.168.2.2`

Object Database Configuration
To activate the overlapping NAT feature, use the `dbedit` database editor GUI (or command line utility). In the sample network configuration, the per interface values for interface A and interface B are set in the following way:

**Sample Network Configuration: Interface Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_overlapping_nat</td>
<td>true</td>
</tr>
<tr>
<td>overlap_nat_dst_ipaddr</td>
<td>The overlapping IP addresses (before NAT). In the sample network configuration, <strong>192.168.1.0</strong> for both interfaces.</td>
</tr>
<tr>
<td>overlap_nat_src_ipaddr</td>
<td>The IP addresses after NAT. In the sample network configuration, <strong>192.168.20.0</strong> for interface A, and <strong>192.168.30.0</strong> for interface B.</td>
</tr>
<tr>
<td>overlap_nat_netmask</td>
<td>The net mask of the overlapping IP addresses. In the sample network configuration, <strong>255.255.255.0</strong>.</td>
</tr>
</tbody>
</table>
Security Management Behind NAT

The Security Management Server sometimes uses a private IP address (as listed in RFC 1918) or some other non-routable IP address, because of the lack of public IP addresses.

NAT [Static or Hide] for the Security Management Server IP address can be configured in one click, while still allowing connectivity with managed gateways. All gateways can be controlled from the Security Management Server, and logs can be sent to the Security Management Server. NAT can also be configured for a Management High Availability server and a Domain Log Server.

Note - Security Management behind NAT is not supported for deployments where the Security Management Server also acts as a gateway and must be addressed from outside the NATed domain, for example, when it receives SAM commands.

In a typical Security Management Behind NAT scenario: the Security Management Server is in a network on which Network Address Translation is performed (the “NATed network”). The Security Management Server can control Security Gateways inside the NATed network, on the border between the NATed network and the outside world and outside the NATed network.

In ordinary Hide NAT configurations, connections cannot be established from the external side the NAT A Security Gateway. However, when using Hide NAT on the Security Management Server, gateways can send logs to the Security Management Server.

When using the Security Management behind NAT feature, the remote gateway automatically selects the Security Management address to be addressed and simultaneously applies NAT considerations.

To enable NAT for the Security Management Server:

• From the NAT page of the Security Management Server object, define NAT and select Apply for A Security Gateway control connections.

Non-Corresponding Gateway Addresses

Sometimes the gateway contacts the Security Management Server with an address that does not correspond to the remote gateway’s deployment, for example:

• When the gateway’s automatic selection does not conform with the routing of the gateway’s deployment. In this case, define the masters and loggers manually, to allow the remote gateway to contact the Security Management Server using the required address. When an inbound connection from a managed gateway enters the Security Gateway, port translation is used to translate the hide address to the real IP address of the Security Management Server.

To define masters and loggers, select Use local definitions for Log Servers and Use local definitions for Masters and specify the correct IP addresses on the gateway.
This solution encompasses different scenarios:

- The remote gateway addresses the NATed IP when you want it to address the real IP.
- The remote gateway addresses the real IP when you want it to address the NATed IP. In this case, specify the SIC name of the Security Management Server in the masters file.

Notes:

- Only one object can be defined with these settings, unless the second object is defined as a Secondary Security Management Server or as a Domain Log Server.
- Ensure that you properly define the Topology settings on all gateways. All workarounds required for previous versions still function with no changes in their behavior.

**Configuring the Security Management Server Object**

To configure the Security Management Server object:

1. From the NAT page on the Primary_Security_Management object, select either Static NAT or Hide NAT. If using Hide NAT, select Hide behind IP Address, for example, 192.168.55.1. Do not select Hide behind Gateway (address 0.0.0.0).
2. Select Install on Gateway to protect the NATed objects or network. Do not select All.

**Configuring the Security Gateway Object**

To configure the Security Gateway object:

2. In the General tab in the Interface Properties window, define the IP Address and the Net Mask.
3. In the Topology tab of the Interface Properties window, select Network defined by the interface IP and Net Mask.

**IP Pool NAT**

An IP Pool is a range of IP addresses (an address range, a network or a group of one of these objects) that is routable to the gateway. IP Pool NAT ensures proper routing for encrypted connections for the following two connection scenarios:

- SecuRemote client / SecureClient to MEP (Multiple Entry Point) gateways
- Gateway to MEP gateways

When a connection is opened from a SecuRemote client / SecureClient or a client behind a gateway to a server behind the MEP Gateways, the packets are routed through one of the MEP gateways. Return packets in the connection must be routed back through the same gateway in order to maintain the connection. To ensure that this occurs, each of the MEP gateways maintains a pool of IP addresses that are routable to the gateway. When a connection is opened to a server, the gateway substitutes an IP address from the IP pool for the source IP address. Reply packets from the server return to the gateway, which restores the original source IP address and forwards the packets to the source.

The pool of IP addresses is configured in the IP Pool page of the gateway object.
**IP Pool Per Interface**

You can define a separate IP address pool on one or more of the gateway interfaces instead of defining a single pool of IPs for the gateway.

Defining an IP pool per interface solves routing issues that occur when the gateway has more than two interfaces. Sometimes it is necessary that reply packets return to the gateway through the same gateway interface. The following illustration shows one of the MEP Gateways in a SecuRemote client / SecureClient to MEP (Multiple Entry Point) gateway deployment.

If a remote client opens a connection to the internal network, reply packets from hosts inside the internal networks are routed to the correct gateway interface through the use of static IP pool NAT addresses.

The remote VPN client’s IP address is NATed to an address in the IP pool on one of the gateway interfaces. The addresses in the IP pool can be routed only through that gateway interface so that all reply packets from the target host are returned only to that interface. Therefore, it is important that the IP NAT pools of the interfaces do not overlap.

When the packet returns to the gateway interface, the gateway restores the remote peer’s source IP address.

The routing tables on the routers that lie behind the gateway must be edited so that addresses from a gateway IP pool are returned to the correct gateway interface.

Switching between IP Pool NAT per gateway and IP Pool NAT per interface and then installing the security policy deletes all IP Pool allocation and all NATed connections.
**NAT Priorities**

IP Pool NAT can be used both for encrypted (VPN) and non-encrypted (decrypted by the gateway) connections.

---

**Note** - To enable IP Pool NAT for clear connections through the gateway, configure INSPECT changes in the `user.def` file. Contact Check Point Technical Support.

For non-encrypted connections, IP Pool NAT has the following advantages over Hide NAT:

- New back connections (for example, X11) can be opened to the NATed host.
- User-to-IP server mapping of protocols that allow one connection per IP can work with a number of hosts instead of only one host.
- IPsec, GRE and IGMP protocols can be NATed using IP Pool NAT (and Static NAT). Hide NAT works only with TCP, UDP and ICMP protocols.

Because of these advantages, you can specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.

The order of NAT priorities are:

1. Static NAT
2. IP Pool NAT
3. Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

---

**Reusing IP Pool Addresses For Different Destinations**

IP Pool addresses can be reused for different destinations, which makes more efficient use of the addresses in the pool. If a pool contains N addresses, then any number of clients can be assigned an IP from the pool as long as there are no more than N clients per server.

Using IP Pool allocation per destination, two different clients can receive the same IP from the pool as long as they communicate with different servers. When reusing addresses from the IP Pool, back connections are supported from the original server only. This means that connections back to the client can be opened only from the specific server to which the connection was opened.

---

The default **Do not reuse IP Pool** behavior means that each IP address in the IP Pool is used once (connections 1 and 2 in the following illustration). In this mode, if an IP pool contains 20
addresses, up to 20 different clients can be NATed and back connections can be opened from any source to the client.

Switching between Reuse and Do not reuse modes and then installing the security policy, deletes all IP Pool allocations and all NATed connections.

**Configuring IP Pool NAT**

To configure IP Pool NAT:

1. In the Global Properties > NAT page, select Enable IP Pool NAT and the required tracking options.
2. In the gateway General Properties page, ensure the gateway version is specified correctly.
3. For each gateway or gateway interface, create a network object that represents its IP pool NAT addresses. The IP pool can be a network, group, or address range. For example, for an address range, do the following:
   a) In the network objects tree, right-click Network Objects branch and select New > Address Range The Address Range Properties window opens.
   b) In the General tab, enter the first and last IP of the address range.
   c) Click OK. The new address range appears in the Address Ranges branch of the network objects tree.
4. Select the gateway object, access the Gateway Properties window and select NAT > IP Pool NAT.
5. In the IP Pool NAT page, select one of the following:
   a) Allocate IP Addresses from and then select the address range you created to configure IP Pool NAT for the whole gateway, or
   b) Define IP Pool addresses on gateway interfaces to configure IP Pool NAT per interface.
6. If required, select one or more of the following options:
   a) Use IP Pool NAT for VPN client connections
   b) Use IP Pool NAT for gateway to gateway connections
   c) Prefer IP Pool NAT over Hide NAT to specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.
7. Click Advanced.
   
a) **Return unused addresses to IP Pool after**: Addresses in the pool are reserved for 60 minutes [default], even if the user logs off. If the user disconnects from their ISP and then redials and reconnects, there will be two Pool NAT addresses in use for the user until the first address from the IP Pool times out. If users regularly lose their ISP connections, you may want to decrease the time-out to prevent the IP Pool from being depleted.

b) **Reuse IP addresses from the pool for different destinations**: This is a good option unless you need to allow back connections to be opened to clients from any source, rather than just from the specific server to which the client originally opened the connection.

8. Click **OK**.

9. Edit the routing table of each internal router so that packets with an IP address assigned from the NAT pool are routed to the appropriate gateway or, if using IP Pools per interface, the appropriate gateway interface.

**IP Pool NAT for Clusters**

IP Pools for gateway clusters are configured in two places in SmartDashboard:

- In the gateway Cluster object **NAT > IP Pool NAT** page, select the connection scenario.
- In the Cluster member object **IP Pool NAT** page, define the IP Pool on the cluster member. A separate IP pool must be configured for each cluster member. It is not possible to define a separate IP Pool for each cluster member interface.
Monitoring Important Events with SmartEvent

The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartEvent consolidates and shows all security events that are generated by these Software Blades:

- Firewall
- Identity Awareness, and URL Filtering
- IPS
- Application Control
- Anti-Bot, Threat Emulation, and Anti-Virus
- DLP

Administrators can quickly identify very important security events and do the necessary actions to prevent more attacks.
For more information about using SmartEvent, see the *R77 SmartEvent Administration Guide*

**Enabling SmartEvent**

To enable SmartEvent on the Security Management Server:

1. In SmartDashboard from the **Network Objects** navigation tree, double-click the Security Management Server or Domain Log Server.
   
   The **General Properties** window opens.

2. In the **Management** tab, select these Software Blades:
   
   • **Logging & Status**
   • **SmartEvent Server**
   • **SmartEvent Correlation Unit**

3. Click **OK**.

4. From the menu bar, select **Policy > Install Database**.

5. From the menu bar, select **SmartConsole > SmartEvent**.

The SmartEvent console opens.

**Creating Reports**

SmartEvent lets you create reports that summarize events for the supported Software Blades. These reports can help you identify attack trends and the effectiveness of the Firewall Rule Base and the security policy. The reports can be automatically sent as emails and PDF files at regular intervals.

To create a SmartEvent report:

1. In SmartEvent, click the **Reports** tab.

2. From the navigation tree, click **All** or a Software Blade.

3. Select the report.
A sample report is shown in the window.

4. Click **Generate**.
   
   The report is generated and shown in a new window.

5. To create a PDF file, click **.**
   
   The report is saved to a PDF.

**Sample Application Control and URL Filtering Event Analysis**

This is a sample procedure that shows how to use SmartEvent to do an analysis of Internet browsing events from the Application Control and URL Filtering Software Blade.

**To show an Internet browsing event:**

1. From SmartEvent **Overview** tab, in the **View** section, click the Application Control and URL Filtering icon.
   
   The Application Control and URL Filtering **Overview** page opens.

2. In **Timeline View**, click the **High Risk** events for a day.
The **High Risk** window opens.

This is some of the information about the event:

- Five users tried to access the VTunnel web proxy
- VTunnel is classified as a **High** security risk and is a Web proxy site that lets users go to websites anonymously
- The names of the 5 users that tried to go to the VTunnel website are shown

### Monitoring Traffic and Connections with SmartLog

The SmartLog Software Blade is a log management tool that reads logs from all Software Blades on Security Management Servers and Security Gateways. SmartLog works with the SmartLog Index Server that gets log files from different log servers and indexes them. SmartLog supplies these monitoring features:

- Quickly search through billions of logs with simple search strings
- Select from many default search queries to find the applicable logs
- Monitor logs from administrator activity and connections in real-time
Enabling SmartLog

The SmartLog Index Server contains a central index of log entries from all SmartLog enabled Security Management Server and Log Servers.

To enable SmartLog:

1. Open SmartDashboard.
2. From the Network Objects tree, double-click the Security Management Server or Domain Log Server.
   The General Properties window opens.
3. In the Management tab, select Logging & Status.
4. From the navigation tree, click Logs.
5. Select Enable SmartLog and then click OK.
6. From the menu bar, select Policy > Install Database.
   The SmartLog Index Server is installed on the Security Management Server.
7. From the menu bar, select SmartConsole > SmartLog.
   The SmartLog console opens.

For more about using SmartLog, see the R77 SmartLog Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=24814.
Sample Log Analysis

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

To show a log of a dropped connection:

1. From SmartLog, in the Query Top Results pane select Top Actions > Drop. The Results pane shows the logs for dropped connections.
2. Double-click a log. The Log Details window opens.

This is some of the information about the dropped connection in the log:
- A telnet connection from 10.6.20.54 to 10.17.45.125 was dropped
- The connection matched rule number 2 (Telnet not allowed) in the Firewall Rule Base
In This Section:

Configuring Fragmentation for IPSec Traffic ............................................................ 129
Configuring Subnet Range Selection for Quick Mode IDs ......................................... 130
Configuring Alternate CRL Distribution Points ....................................................... 130
Configuring Fail Open When CRL is Unavailable ................................................... 130
Configuring Persistent VPN Kernel Parameters ..................................................... 131
Disabling IKEv2 Traffic Selector Narrowing ......................................................... 131
Configuring the GTP Signaling Rate Limit ............................................................... 131
Configuring GTPv2 Support ..................................................................................... 132
Configuring SCTP Inspection .................................................................................. 133
Configuring GSN Handover Group Limits ............................................................... 135
DeactivatingSession Hijacking Protection ............................................................. 136
Using Diameter Services in Rules ......................................................................... 136
Sending Check Point Logs to a Syslog Server ........................................................ 141
Configuring CGNAT ............................................................................................... 143
Configuring Stateful NAT64 ................................................................................ 144
Large Scale VPN .................................................................................................... 146
Configuring New GTPv2 Message Types and Information Elements ...................... 147

**LTE**

In This Section:

Configuring Fragmentation for IPSec Traffic ............................................................ 129
Configuring Subnet Range Selection for Quick Mode IDs ......................................... 130
Configuring Alternate CRL Distribution Points ....................................................... 130
Configuring Fail Open When CRL is Unavailable ................................................... 130
Configuring Persistent VPN Kernel Parameters ..................................................... 131
Disabling IKEv2 Traffic Selector Narrowing ......................................................... 131
Configuring the GTP Signaling Rate Limit ............................................................... 131
Configuring GTPv2 Support ..................................................................................... 132
Configuring SCTP Inspection .................................................................................. 133
Configuring GSN Handover Group Limits ............................................................... 135
Deactivating Session Hijacking Protection ............................................................. 136
Using Diameter Services in Rules ......................................................................... 136
Sending Check Point Logs to a Syslog Server ........................................................ 141
Configuring CGNAT ............................................................................................... 143
Configuring Stateful NAT64 ................................................................................ 144
Large Scale VPN .................................................................................................... 146
Configuring New GTPv2 Message Types and Information Elements ...................... 147

LTE is supported on Gaia Security Gateways of R77.30 and higher, and requires the R77.30 Add-On ([see sk105412 http://supportcontent.checkpoint.com/solutions?id=sk105412](http://supportcontent.checkpoint.com/solutions?id=sk105412)) on the Security Management Server or Multi-Domain Server.

**Configuring Fragmentation for IPSec Traffic**

To make sure the size of the transmitted packets is less than the MTU size, configure fragmentation for IPSec traffic.

**To configure fragmentation for IPSec traffic:**

1. On the management server (Security Management Server or Multi-Domain Server) command line, run `dbedit` in Expert mode.
2. At the `dbedit` prompt, run:
   ```
   modify network_objects gateway_object VPN:ipsec_fragment_inner true
   ```
3. Enter `-q` to close `dbedit`.
4. Reboot the server.
5. Install policy.

**To configure fragmentation for IPSec traffic when using Performance Pack:**

1. On each Security Gateway, open the file `$PPKDIR/boot/modules/simkern.conf` in a text editor.
   **NOTE:** If the file does not exist, create it.
2. Add this line: `vpn_f2f_for_fragmentation=1`
3. Save and close the file.
4. Reboot the gateway.

## Configuring Subnet Range Selection for Quick Mode IDs

In Quick Mode, you can apply the subnet range selection specified through `max_subnet_for_range` to the ID of the local gateway, to a peer’s ID, to both, or to none.

**To configure the subnet range selection for Quick Mode IDs:**

On each Security Gateway, run this command:

```
fw ctl set int <subnet_for_range_control> [0|1|2|3] VPN
```

These are the options for the `subnet_for_range_control` value:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><code>max_subnet_for_range</code> table is ignored on both sides.</td>
</tr>
<tr>
<td>1</td>
<td><code>max_subnet_for_range</code> table is ignored when own source IDs are selected.</td>
</tr>
<tr>
<td>2</td>
<td><code>max_subnet_for_range</code> table is ignored when peer’s destination IDs are selected.</td>
</tr>
<tr>
<td>3</td>
<td>The default: <code>max_subnet_for_range</code> table is never ignored.</td>
</tr>
</tbody>
</table>

## Configuring Alternate CRL Distribution Points

For a CA domain, with certificate revocation information distributed to CRL Distribution Points, configure each CA to access these Distribution Points.

**To configure alternate CRL Distribution Points for a CA server:**

1. On the management server (Security Management Server or Multi-Domain Server) command line, run `dbedit` in Expert mode.
2. At the `dbedit` prompt, run this command for each CA:
   ```
addelement servers <ca_server_name> forced_crl_dp <Distribution_Point_URL>
```
   **Example:** `addelement servers MyCA forced_crl_dp http://mydomain.com/crlfile1.CRL`
3. Enter `-q` to close `dbedit`.
4. Reboot the server.
5. Install policy.

**NOTE:** You can assign several CRL DPs for each CA server.

## Configuring Fail Open When CRL is Unavailable

By default, if a CRL is unavailable, the VPN connections that rely on it for the certificate verification shut down. To maintain network availability during a CRL failure, you can configure the Fail-Open mode on the gateways.
To configure Fail-Open:

1. On the management server (Security Management Server or Multi-Domain Server) command line, run `dbedit` in Expert mode.
2. At the dbedit prompt, run:
   ```
   modify network_objects gateway_object VPN:ike_fetch_crl_fail_open true
   ```
3. Enter `-q` to close dbedit.
4. Reboot the server.
5. Install policy.

   **Note** - In Fail-Open mode, if the CRL is not available or is not readable, the certificate is not examined for possible revocation.

### Configuring Persistent VPN Kernel Parameters

If you change VPN kernel parameters (usually with `fw ctl set`), they return to their default values after reboot. If you configure persistent VPN kernel parameters, those changes stay.

To configure persistent VPN kernel parameters:

1. On the Security Gateway, create this file:
   ```
   $FWDIR/modules/vpnkern.conf
   ```
2. Add the required parameter(s) to `vpnkern.conf`.
3. **Example**: `subnet_for_range_control=2`
4. Save the file.
5. Reboot the gateway.

### Disabling IKEv2 Traffic Selector Narrowing

During IKEv2 SA negotiation, the responder can narrow the traffic selector proposed by the initiator. You can disable this feature.

To disable IKEv2 Traffic Selector Narrowing with dbedit:

1. On the management server (Security Management Server or Multi-Domain Server) command line, run `dbedit` in Expert mode.
2. At the dbedit prompt, run:
   ```
   modify network_objects gateway_object VPN:ikev2_accept_all_ts true
   ```
3. Enter `-q` to close dbedit.
4. Reboot the server.
5. Install policy.

### Configuring the GTP Signaling Rate Limit

The Security Gateway calculates the maximum signal rate. It multiplies the value of GTP Signaling rate limit sampling interval and the value of GTP signal packet rate limit. To configure the GTP signaling rate, configure these properties.
To configure GTP signaling rate limit:

1. Create one or more groups of source network objects.
   a) In SmartDashboard, right-click **Network Objects** and select **Groups > GSN Handover Group**.
   b) In the **GSN Handover Group Properties** window enter:
      - **Name** - Unique character string identifier
      - **Comment** (optional) - Descriptive text
      - **Color** (optional) - Select a color for the group icon
   c) Select **Enforce GTP signal packet rate limit from this group** and enter an integer value (in PDU/sec).
   d) From the **Not in Group** list, double-click the network objects to be included in the group.
   e) Click **OK**.

2. Configure the sampling interval.
   a) In SmartDashboard, click **Edit Global Properties**.
      The **Global Properties** window opens.
   b) In the navigation tree, click **Firewall-1 GX**.
   c) Enter an integer for **GTP Signaling rate limit sampling interval** (in seconds).
      Default = 1 second.
   d) Click **OK**.

3. Install policy.

Configuring GTPv2 Support

You can create **Firewall** rules with GTPv2 protocol services for S5/S8 LTE interfaces. You can use these new GTPv2 services in the **Service** column of rules.

**Note** - There is no service template for the **Path Management GTPv2** service. You must manually create the template.

To create a GTPv2 service (Not including Path Management):

1. In SmartDashboard, go to the **Firewall** tab and select the **Services** tree.
2. Right-click **GTP** and select **New GTP**.
3. Select a service template from the options menu:
   • **GTP V2** – for Tunnel Management service
   • **GTP Mobility Management V2** – for Mobility Management service
   • **GTP V2 Additional** – Custom defined service
4. In the **Services Properties** window, enter a name for the new service.
5. If you selected the **GTP V2 Additional** service, select one or more service types:
   • **GTPv2 Trace Management**
   • **CS Fallback and SRVCC**
   • **Restoration and Recovery services**
Note - GTP-U messages cannot match GTPv2 services in Firewall rules. You must also include the GTPv1 service in the rule to match GTP-U messages.

To create the Path Management GTPv2 service:

1. On the Firewall tab, right click Services.
2. Right-click Other > New Other.
3. In the Other Services Properties window, enter this string as the service name: gtpv2_path_mgmt
4. Enter 17 in the IP Protocol field.
5. Click Advanced.
6. In the Advanced Other Service Properties window, enter this string in the Match field: gtp_path_match_v2
7. Select the Accept Replies option.

Configuring SCTP Inspection

When a Carrier license is installed, you can specify SCTP services in your Firewall rules. SCTP Inspection occurs in these cases:

- There is a match on a rule containing an SCTP or Diameter SCTP service in the Service cell.
- There is a match on a rule with Service = Any and this SCTP service has Match for any selected.

To activate SCTP Inspection:

1. Open SmartDashboard > Manage.
2. Click Services > New > SCTP.
   The SCTP Service Properties window opens.
   - Name - The name of the service. The name assigned here must be the same as the server service name (as in the services file). If NIS is used, the firewall automatically retrieves the information from NIS.
   - Port - The number of the port that gives this service.
   - Keep connections open after policy has been installed - If the connections are not allowed in the new policy, they are still kept. This overrides the settings in the Connection Persistence page. If you change this property, the change does not have effect on open connections, but only future connections.
3. Click Advanced.
   The Advanced SCTP Service Properties window opens.
   - Source Port - Port number for the client side service. If specified, only those Source port Numbers will be Accepted, Dropped, or Rejected during packet inspection. Otherwise, the source port is not inspected.
   - Enable Aggressive Aging - Sets short (aggressive) timeouts for idle connections. When a connection is idle for more than its aggressive timeout value, it is marked as eligible for deletion. When memory consumption or connections table capacity exceeds a user-defined threshold (high watermark), aggressive aging starts. Each incoming connection starts to delete $k$ (10 by default) connections that are eligible for deletion. This continues until memory consumption or connections capacity decreases below the low value.
- **Synchronize connections on cluster** - Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with **Synchronize connections on cluster** selected are synchronized as they go through the cluster. By default, all new and existing services are synchronized.

4. Click **OK**.

5. Open **Global properties > Stateful Inspection**.

Configure these **Stateful Inspection** options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| SCTP start timeout    | - An SCTP connection times out if the interval between the arrival of the first packet and establishment of the connection (STCP four-way handshake) exceeds the SCTP start timeout in seconds.  
  - Attribute name in GuiDBedit: `sctpstarttimeout` |
| SCTP session timeout  | - Length of time an idle connection remains in the Security Gateway connections table.  
  - Attribute name in GuiDBedit: `sctptimeout` |
| SCTP end timeout      | - A SCTP connection will only terminate SCTP end timeout seconds after two FIN packets (one in each direction: client-to-server, and server-to-client) or an RST packet.  
  - Attribute name in GuiDBedit: `sctpendtimeout` |

Configure these options for **Out of state packets**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| Drop out of state SCTP packets | - Drop SCTP packets that are not consistent with the current state of the SCTP connection.  
  - Attribute name in GuiDBedit: `fw_drop_out_of_state_sctp` |
| Log on drop           | - Generates a log entry when out of state SCTP packets are dropped.  
  - Attribute name in GuiDBedit: `fw_log_out_of_state_sctp` |

To deactivate out of state packet drop with SmartDashboard:

1. In SmartDashboard, go to **Global properties > Stateful Inspection**.
2. Clear the **Drop out of state SCTP packets** option.
3. Save and install the policy.

To deactivate packet inspection with GuiDBEdit:

1. Open **GuiDBedit**.
2. Search for: `fw_sctp_packet_inspection`.
3. Set the property to **false**.
4. Save the database and install policy.

**Configuring SCTP Acceleration**

To enable SCTP acceleration:

```
sim feature sctp on
```
To disable SCTP acceleration, run: `sim feature sctp off`

**Note:** If SCTP acceleration is activated and SCTP inspection is deactivated, the Performance Pack accelerates all SCTP packet types.

### Configuring SCTP NAT

SCTP NAT overrides the defined NAT policy. When this feature is not activated, SCTP connections do not use NAT.

**To activate SCTP NAT:**

On the Security Gateway, run: `fw ctl set int fwx_enable_sctp_nat 1`

**To deactivate SCTP NAT:** `fw ctl set int fwx_enable_sctp_nat 0`

### Configuring GSN Handover Group Limits

You can specify tunnel limits, for GTP handover groups. A newly created tunnel counts against the limit for handover groups on both sides of the tunnel.

**To configure GSN handover group limits:**

1. Run `GuiDBedit` and connect to the management server.
2. Search for `gtp_groups_limit_enabled` and set the value to `true`.
   - Search for `gtp_group_percentage_limit` and set the value to an integer that defines the percentage (0 - 100) of the tunnel capacity assigned to all handover groups.
   - The default value is 0 (unlimited).
   - This percentage applies to all groups for which no limit is defined explicitly.
3. Search for `gtp_tunnels_limit`.
   - This parameter is the maximum number of GTP tunnels that a handover group can create. Set this limit to make sure that one group does not take too much of the GTP tunnel allowance.
4. Search for `gtp_tunnel_group_limit` in each handover group.
   - This value is an integer that defines the maximum number of tunnels that can be open for the specified group. The default value is 0 (not defined).
   - The explicitly defined `gtp_tunnel_group_limit` has precedence over the `gtp_groups_percentage_limit` definition.

### Monitoring GSN Handover Group Limits

This command shows tunnel use for handover groups. Run it in Expert mode on the Security Gateway.
Syntax
fw gtp ho_groups {-g <name> | -l} [-m <lines>] [-s { name | tunnels | limit | util }] [-r]}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-g &lt;name&gt;</td>
<td>Show only the specified handover group</td>
</tr>
<tr>
<td>-l</td>
<td>Show only the handover group names (no data)</td>
</tr>
<tr>
<td>-m &lt;lines&gt;</td>
<td>Show, at most, the specified number of lines</td>
</tr>
<tr>
<td>-s</td>
<td>Sort the output by tunnel name, assigned limit or tunnel utilization</td>
</tr>
<tr>
<td>-r</td>
<td>Sort the output in in reverse alphabetical order</td>
</tr>
</tbody>
</table>

Example
# fw gtp ho_groups
Name                            Open tunnels      Limit %Utilization
------------------------------- ------------ ---------- ------------
Operator-6-GSNs                        25000     100000           25
Operator-9-GSNs                        33148      50000           66
Operator-3-GSNs                          380      no limit          n/a
Operator-8-GSNs                        15897     200000            7
Operator-5-GSNs                        84125     180000           46
Operator-4-GSNs                            0      50000            0
Operator-1-GSNs                        45000      45000          100
Operator-7-GSNs                        69716      70000           99
Operator-2-GSNs                       394326     500000           78

Deactivating Session Hijacking Protection

The Session Hijacking protection is turned on by default. You can deactivate it with one command.

To deactivate the Session Hijacking protection, run this command on the Security Gateway in Expert mode:

# fw ctl set int gtp_allow_ho_bypass 1

To re-activate Session Hijacking protection, run:

# fw ctl set int gtp_allow_ho_bypass 0

Using Diameter Services in Rules

Diameter inspection rules examine traffic for Diameter application compatibility and compliance with the applicable protocols. If the inspection detects an error or incompatibility, the traffic is always dropped.

You can create Firewall rules that inspect Diameter traffic based on matching Diameter services. Each Diameter service is related to a Diameter application (on page 11), which must support the Diameter base protocol. This release includes some predefined Diameter applications. You can create your own custom Diameter applications (“Creating Diameter Applications” on page 139) as necessary.
You must define Diameter services for use in rules. You can define services for Diameter over SCTP or Diameter over TCP.

**Notes and Limitations:**

- All Diameter inspection rules must use the **Accept** action. Do not use the **Drop** or **Reject** actions, because this can cause valid Diameter traffic to be dropped.
- You can include Diameter SCTP and Diameter TCP services in the same rule, or create different rules for each.
- When a rule has same source and destination objects, you must include all applicable Diameter services in one rule. You cannot use more than one rule with the same source and destination for different Diameter services. This can cause valid Diameter traffic to be dropped.

**Creating Diameter SCTP Services**

**To Create a Diameter SCTP Service:**

1. Open **SmartDashboard**.
2. On the **Firewall** tab, open **Services** objects tree.
3. Right-click **Services**.
4. Select **Diameter > New Diameter SCTP**.
   
   The **Diameter SCTP Service Properties** window opens.

   - **Name** - The name of the service. The name assigned here must be the same as the server service name (as in the services file). If NIS is used, the firewall automatically retrieves the information from NIS.
   - **Comment** - Optionally enter a comment.
   - **Color** - Select a color.
   - **Application** - Select a Diameter application. If the required application is not in the list, you can create a new one ("Creating Diameter Applications" on page 139).
   - **Keep connections open after policy has been installed** -Overrides the settings defined on the **Connection Persistence** page. If you change this parameter, the change does not apply to existing open connections.

5. Click **Advanced**.
   
   The **Advanced SCTP Service Properties** window opens.

6. Configure these parameters.

   - **Source Port** - Port number for the client side service. If specified, only those Source port Numbers will be Accepted, Dropped, or Rejected during packet inspection. Otherwise, the source port is not inspected.
   - **Enable Aggressive Aging** - Sets short (aggressive) timeouts for idle connections. When a connection is idle for more than its aggressive timeout value, it is marked as eligible for deletion. When memory consumption or connections table capacity exceeds a user-defined threshold (high watermark), aggressive aging starts. Each incoming connection starts to delete k (10 by default) connections that are eligible for deletion. This continues until memory consumption or connections capacity decreases below the low value.
   - **Synchronize connections on cluster** - Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster. Of the services allowed by the Rule Base, only those with **Synchronize connections on cluster** selected are synchronized as they go through the cluster. By default, all new and existing services are synchronized.
7. Click **OK** two times to close the windows.

See the Rule limitations ("Using Diameter Services in Rules" on page 136). Use SmartView Tracker to see connections that use SCTP services.

**Creating Diameter TCP Services**

To Create a Diameter TCP Service:

1. Open **SmartDashboard**.
2. On the **Firewall** tab, open **Services** objects tree.
3. Right-click **Services**.
4. Select **Diameter > Diameter TCP**. 
   
   The **Diameter TCP Service Properties** window opens.

   - **Name** - The name of the service. The name assigned here must be the same as the server service name (as in the services file). If NIS is used, the firewall automatically retrieves the information from NIS.
   - **Comment** - Optionally enter a comment.
   - **Color** - Select a color.
   - **Application** - Select a Diameter application. If the required application is not in the list, you can create one ("Creating Diameter Applications" on page 139).
   - **Keep connections open after policy has been installed** - Overrides the settings defined on the **Connection Persistence** page. If you change this parameter, the change does not apply to existing open connections.

5. Click **Advanced**.

   The **Advanced TCP Service Properties** window opens. Configure these parameters.

   - **Source Port** - Port number for the client side service. If specified, only those Source port Numbers will be Accepted, Dropped, or Rejected during packet inspection. Otherwise, the source port is not inspected.
   - **Enable for TCP Resource** - Enables the TCP service for a TCP Resource.
   - **Match for Any**. - If selected, this service is used when ‘Any’ is set for the rule’s service and there are several service objects with the same source port and protocol.
   - **Session Timeout** - Time (in seconds) before the session times out.
     - **Default** - Use the default value defined on the Stateful Inspection page in **Global Properties**.
     - **Other** - Manually define a timeout period for this service.
   - **Enable Aggressive Aging** - Sets short (aggressive) timeouts for idle connections. When a connection is idle for more than its aggressive timeout value, it is marked as *eligible for deletion*. When memory consumption or connections table capacity exceeds a user-defined threshold (high watermark), aggressive aging starts. Each incoming connection starts to delete \( k \) (10 by default) connections that are eligible for deletion. This continues until memory consumption or connections capacity decreases below the low value.
   - **Synchronize connections on cluster** - Enables state synchronization on a ClusterXL or OPSEC-certified cluster.
   - **Perform static NAT good port selection on Cluster** - All traffic inspection for a connection is done by the same cluster member. This option makes for better connection stickiness.

6. Click **OK** two times to close the windows.
Creating Diameter Applications

You can create custom Diameter applications to use in Diameter services. Custom Diameter applications are typically related to an RFC. Each application includes one or more Diameter commands.

**Note** - This advanced feature is complex and requires detailed knowledge of the Diameter protocols. We recommend that you coordinate use of this feature with Check Point support.

To create a Diameter application:

1. Open GuiDBedit.
2. On the Tables tab open Other and select diameter_service_cfg.
3. Click in the Object pane.
4. Click Object > New.
   
   The Create Object window opens.
   
   - Class - select diameter_app.
   - Object - enter the name of the new application.
   - Click OK.
   
   The new object is added to list of objects and its fields show in the bottom pane of GuiDBedit.

5. In Field Name column (in the lower pane in the window):
   
   a) Double-click app_cmds.
      
      The Add/Edit Element window opens.
   
   b) Select an application command from the Object list.
      
      If the command does not exist, create it (“Creating Diameter Application Commands” on page 140).
      
      Repeat steps a. and b. as necessary to add more application commands.
   
   c) Double-click app_id.
      
      The Edit window opens.
   
   d) Enter a value for the application id.
      
      The app_id must be the same id as in the RFC for this application.
   
   e) Double-click include_diameter_base_app.
      
      Make sure the value is true, unless you want to block some application commands (“Blocking Specified Application Commands” on page 141).
   
   f) Double-click is_diameter_base_app.
      
      Make sure the value is false.

6. Save and close GuiDBedit.

In SmartDashboard, the new application shows in the Diameter TCP/SCTP Service Properties window. You must restart SmartDashboard before you can use the new service in a policy rule.
Creating Diameter Application Commands

A Diameter application includes one or more commands. There are default commands, and you can create new request or answer commands.

**Note** - This advanced feature is complex and requires detailed knowledge of the Diameter protocols. We recommend that you coordinate use of this feature with Check Point support.

To create a Diameter application command:

1. In GuiDBedit, click in the **Object Name** column.
2. Click **Objects > New**.
   
The Create Object window opens.
3. From **Class** select **diameter_cmd**.
   
   **Note** - **diameter_avp** is not a valid option creating Diameter Application commands. The **diameter_avp** option is used only for creating **diameter_avp** objects and is not enforced by the policy.
4. In the **Object** field, enter a name for the new command.
   
   - Use the application command names as defined by the applicable RFC.
   
   - Select the request or answer command as necessary. For example, **new_cmd_request** or **new_cmd_answer**.
5. Click **OK**.
   
The new command shows in the **Objects** table.
6. Select the new command.
7. In the **Field** table:
   
   a) Double-click **cmd_code**.
      
      In the **Edit** window, enter the value specified by the related RFC.
      
      Click **OK**.
   
   b) Double-click **display_code**.
      
      In the **Edit** window, enter the value specified by the related RFC (a three-letter code, for example NCR or NCA).
      
      Click **OK**.
   
   c) Double-click **request**.
      
      In the **Edit** window, select **true** or **false**:
      
      - Application **request** commands must be **true**.
      
      - Application **answer** commands must be **false**.
8. Click **OK**.
9. On the toolbar, click the **Save all changed objects** button.

**Important** - You must save new commands before you can add them to a diameter application.
Blocking Specified Application Commands

You can create a service for an application that excludes specified commands. This lets you use a Diameter rule to block traffic that uses the specified commands.

Note - This advanced feature is complex and requires detailed knowledge of the Diameter protocols. We recommend that you coordinate use of this feature with Check Point support.

In a Diameter application, the `include_diameter_base_app` value is typically set to `TRUE`. To block commands allowed by the base protocol:

1. Create a custom Diameter application with an ID that is not related to an RFC.
   - Add only the commands to be allowed.
   - Set the `include_diameter_base_app` property to `FALSE`.
2. Create a new service that uses the new custom Diameter application, for SCTP “Creating Diameter SCTP Services” on page 137 or TCP inspection “Creating Diameter TCP Services” on page 138.
3. Add the new Service to a Diameter rule.
4. Install policy.

Notes and limitations:

- Make sure the source and destination Diameter nodes use the custom application. If not, the rule will not exclude the blocked application commands because it will use the standard RFC based application.
- All Diameter Services rules must have the `include_diameter_base_app` property set to the same value - `FALSE`. If not, the rule will not exclude the blocked application commands because it will use the standard RFC based application.

Sending Check Point Logs to a Syslog Server

By default, gateway logs are sent to the Security Management Server. You can configure gateways to send logs directly to syslog servers. First, define syslog servers. Then, update the logging properties of the gateways.

These syslog protocols are supported:

- RFC 3164 [old]
- RFC 5424 [new]

Limitations

- IPv6 logs are not supported
- Software Blade logs are not supported

Defining Syslog Servers

To define a Syslog server:
1. In SmartDashboard, click the Firewall tab.
2. In the Servers and OPSEC Applications object tree, right-click Servers > New > Syslog.
3. In the **Syslog Properties** window, enter or select:
   - Name
   - Optional comment
   - Host
   - Port (Default = 514)
   - Version [BSD Protocol or Syslog Protocol]

```
<81>Jul 25 17:26:49 172.23.22.63 Action="accept" src="91.90.139.74" dst="172.23.22.63" proto="17" product="VPN-1 & FireWall-1" service="1147" s_port="26666" product_family="Network"
```

Example of a **Syslog Protocol** log entry (truncated):

```
<81>1 2012-07-25T17:50Z 172.23.22.63 CP-GW - Log
[Fields@1.3.6.1.4.1.2620 Action="accept" rule="1" src="91.90.139.74" dst="172.23.22.63" proto="17" product="VPN-1 & FireWall-1" service="1052" s_port="54444" product_family="Network"]
```

### Configuring Gateways to Send Logs to Syslog Servers

You can configure a gateway to send logs to multiple syslog servers. The syslog servers must be the same type: **BSD Protocol** or **Syslog Protocol**.

To send the logs of a gateway to syslog servers:

1. In SmartDashboard, go to **gateway Properties > Logs**.
2. In the **Send logs and alerts to these log server** table, click the green button to add syslog servers.
   - **Note** - You cannot configure a Syslog server as a backup server.
3. Click **OK**.
4. Install policy.

### Enabling Syslog in Kernel

The `fwsyslog_enable` kernel parameter enables or disables the **Syslog in Kernel** feature:

- **0** = Disabled (default)
- **1** = Enabled

You can enable or disable Syslog in Kernel temporarily (until the system reboots) or permanently (until manually disabled).

**To temporarily enable Syslog in Kernel on a Security Gateway:**

1. Run: `# fw ctl set int fwsyslog_enable 1`
2. Install Policy.

**To permanently enable Syslog in Kernel on a Security Gateway:**

1. Run:
   ```
   echo fwsyslog_enable=1 >> $FWDIR/modules/fwkern.conf
   ```
2. Reboot the Security Gateway or cluster members.

**To disable Syslog in Kernel temporarily:**

Run: `# fw ctl set int fwsyslog_enable 0`
To disable Syslog in Kernel permanently:

1. Open `$FWDIR/modules/fwkern.conf` in a text editor and do one of these actions:
   - Set `fwsyslog_enable=0`
   - Or
   - Delete the `fwsyslog_enable` line.
2. Reboot the Security Gateway.

**Verification**

**To see the Syslog in Kernel status:**

```
[Expert@host:0]# fw ctl get int fwsyslog_enable
```

You can see the count of logs sent to syslog from the kernel. Log counters start when you install the policy.

**To see log count for an instance:**

```
[Expert@host:0]# fw -i <instance_number> ctl get size fwsyslog_nlogs_counter
```

*Sample output:*

```
fwsyslog_nlogs_counter = 21
```

**To see log count for all instances:**

1. Open two command line connections to the Security Gateway.
2. On the first CLI connection, run: 
   ```
   # fw ctl zdebug
   ```
3. On the second CLI connection, run:
   ```
   # fw ctl set size fwsyslog_print_counter 1
   ```
4. On the first shell, see the counter for each instance and the sum of all instances.

*Sample output:*

```
;[cpu_2];[fw4_0];Number of logs sent from instance 0 is 43;
;[cpu_2];[fw4_0];Number of logs sent from instance 1 is 39;
;[cpu_2];[fw4_0];Number of logs sent from instance 2 is 50;
;[cpu_2];[fw4_0];Total fwsyslog_nlogs_counter = 132;
```

**Configuring CGNAT**

**To configure CGNAT objects:**

1. In SmartDashboard, create a subscriber **Network Object**.
   You can use one network object to handle traffic for one subscriber or for many subscribers.
   a) In the **Network Properties** window - **General** tab, enter the IPv4 address and subnet mask in the applicable fields.
   b) Configure other properties as necessary.
2. Create a subscriber **Address Range Object**.
   *Important* - If you cannot define the hide range with one continuous address range, you must divide the subscriber networks into subnets and then create different CGNAT rules for each network segment.
To create a CGNAT Rule:
1. In the NAT pane, create a new rule.
2. Right-click the Translated Packet - Source cell and select Add (Hide CGNAT).
3. In the Add Object window, select the subscriber Address Range Object.
4. In the Original Packet - Source cell, select the subscriber Network Object.
5. Move the cursor over the Translated - Source cell to see the number of ports for each subscriber.
   Important - If the calculated number of ports per subscriber is less than 10, a warning message shows. If this occurs, increase the number of addresses in the hide range.
6. Install Policy.

CGNAT Rule Notes
- Use only IP address range objects for the translated source.
- Do not change the destination and service cell default values.
- Do not use overlapping IP addresses in rules. When rules include overlapping IP address ranges, only the first occurrence of the overlapping address is used.
  For example, if:
  Rule 1 uses ip-range: 10.10.10.1-50
  Rule 2 uses ip-range: 10.10.10.30-100
  Then:
  Rule 1 is applicable to the full range (10.10.10.1-50).
  Rule 2 is applicable only to the sub-range (10.10.10.51-100).

Tracking CGNAT Rule Activity
To use CGNAT to identify the original subscriber IP address:
1. Run SmartLog.
2. Use this query for the address/port combination.
   hide_ip:<public ip> and hide_port:<public port number>
   For example, hide_ip:10.1.1.10 and hide_port:38200.
3. Click a record to see the original subscriber IP address.

Configuring Stateful NAT64
Before you define NAT64 rules:
1. For embedded NAT64, define an address range network object with an IPv4 range.
   This range must be routable and not in use on the IPv4 side of the network. We recommend that you define a large range for more concurrent NAT64 connections.
2. Define IPv6 network objects for your IPv4 hosts:
   - You can define IPv4 embedded IPv6 addresses for servers, IP address ranges and network objects.
   - You can define static IPv6 addresses for servers and other 'simple' host objects.
Defining a NAT64 Rule

Define NAT64 rules as Manual NAT rules in the NAT policy view. Make sure that you add firewall security rules that allow NAT traffic.

Use the standard procedure for NAT rules, with these differences:

1. The Translated Packet Source cell must contain an IPv4 hide range.
2. The Original Packet Destination cell must contain one of these:
   - A supported network object with an IPv4-embedded IPv6 address
   - A host object with one, static IPv6 address
3. You must set the Translation Method to Stateful NAT64. Right-click the Translated Packet Source cell and select ADD > Stateful NAT64.

Notes:

When you set the NAT Method to Stateful NAT64:

- The Translated Packet Destination cell shows Embedded IPv4.
- A 64 icon shows in the Translated Packet Source and Destination cells.
- You can change the contents of the Translated Destination cell if the Original Destination is also a host object. The cell contents can only contain host objects with IPv4 addresses.
- An icon with an S shows that the cell contains a 1:1 static address translation of the destination.
- Make sure the gateway interface to the IPv4 network is configured correctly:
  - There is an IPv6 address assigned to this interface.
  - The network prefix length is equal to or less than 96.
  - The Security Gateway routing table sends traffic for the original IPv6 destination (as defined by the NAT rule) to the IPv4 interface.

Other Settings


We recommend that you change the default settings only if you are familiar with the technology.

**Copy type of service to service class** (Activated by default) - This setting copies the traffic class field to the type of service field, and sets the type of service field in the translated packet to zero.

**PMTU black hole avoidance** (Deactivated by default) - Allows packet fragmentation on the IPv4 [destination] side during PMTU discovery. Activate this setting if some equipment combinations cause PMTU discovery to fail.

**Add UDP checksum** (Deactivated by default) - Lets the translator calculate and add a valid UDP checksum value to a packet if the packet checksum value is zero. This is important because, by default, an IPv4 UDP packet with a checksum value of zero is dropped on the IPv6 side.

Gateway Configuration

Make sure the number of IPv6 firewall instances is equal to the number of IPv4 firewall instances.
Logging

Source and destination IP addresses show in their original IPv6 format. To identify a NAT64 entry, look in the More section of the Record Details window.

XlateSrc - Source hide IPv4 address
XlateDst - Destination embedded IPv4 address
Information - Identifies the entry as NAT64 traffic

Large Scale VPN

A VPN that connects branch offices, worldwide partners, remote clients, and other environments, can reach hundreds or thousands of peers. A VPN on this scale brings new challenges. For example, when a new peer is deployed in production, you must define the peer and configure the environment again. Every time a new peer is deployed, you must Install Policy on all the Security Gateways.

The Large Scale VPN (LSV) feature addresses these challenges to deploy more easily and quickly. LSV is supported in R77.30 and higher.

To configure Large Scale VPN:

1. If necessary, create a Trusted CA object in SmartConsole for the CA server that signs LSV peer certificates.
2. In SmartConsole, right-click Network Objects > Others and select LSV Profile.
3. In the Large Scale VPN Properties window > General page, enter a unique name for the LSV Profile.
4. Select a Certificate Authority (CA) to sign peer certificates from the list. A CA can sign for only one LSV profile.
5. In the VPN tab, add VPN communities.
6. Optional: In the Advanced tab, define limitations for LSV peers:
   - Limit peer’s VPN Domain size - Set the maximum number of IP addresses in the VPN domain.
   - Allow any - All IP addresses can be included in the VPN domain.
   - Restrict to a group or network - Include only the selected groups or networks in the peer domain.
7. Click OK.
   The LSV Profile is under Network Objects > Interoperable Devices.
   Open SmartDashboard > IPsec VPN > Communities. Double-click the community to which you added the LSV profile, and make sure it is listed with the gateways.
8. Install policy.

Monitoring LSV Peers and Tunnels

You can monitor LSV peers on a Security Gateway with the vpn lsv command.

1. From the Security Gateway command line, run: vpn lsv
2. Select an option.

********** Select Option **********

(1) List all LSV peers
(2) Show LSV peer's details
(3) Remove an LSV peer
(4) Remove all LSV peers
(Q) Quit

You can also monitor LSV tunnels with SmartView Monitor.

Configuring New GTPv2 Message Types and Information Elements

This release lets you add user defined message types and information elements for GTPv2.

- **gtpv2_ignore_messages** - for unknown message types
- **gtpv2_ignore_elements** - for unexpected information elements

The GTPv2 protocol supports user defined information elements (ies) and message types. You can configure Firewall-1 GX to identify these items as legitimate traffic.

To configure Firewall-1 GX to allow these message types and information elements, add these lines to `$FWDIR/lib/gtp.def` on the management server:

- `gtpv2_ignore_messages = {<new_message_types>};`
- `gtpv2_ignore_elements = {<new_information_element_types>};`

Example:

- `gtpv2_ignore_messages = {224,233,251};`
- `gtpv2_ignore_elements = {99,101,103};`

Message types 224, 233, 251 and information elements 99, 101, 103 are allowed by gateway.
Index

A
Access Control and the Rule Base • 16
Action • 66
Activating Single Sign On • 34
AD Query • 50
Adding a Certificate • 71
Adding an Access Role to a Rule • 61
Adding an IPS Exception • 76
Adding Data Owners • 90
Adding Network Exceptions • 76
Adding Users to the Rule Base • 60
Adding Users to the Security Policy • 50
Advanced NAT Settings • 113
Allowing Mobile Connections • 33
Allowing VPN Connections • 47
Analyzing and Tracking DLP • 94
Analyzing the Rule Base (Hit Count) • 26
Anti-Bot • 11
Anti-Bot and Anti-Virus • 80
Anti-Bot and Anti-Virus Rule Base • 82
Anti-Spam • 84
Anti-Virus • 11
APP Wiki • 11
Applications/Sites • 65
Authentication Tab • 59
Automatic and Manual NAT Rules • 105
Automatic and Proxy ARP • 113
Automatic Hide NAT to External Networks • 108

B
Basic Rules • 21
Block • 11
Blocking Specified Application Commands • 142
Bot • 11
Browser-Based Authentication • 51
Browsing IPS Protections • 77

C
CGNAT Rule Notes • 145
Check Point Firewall Security Solution • 14
Check Point Mobile Access Solutions • 29
Check Point Software Acceleration Solutions • 98
Citrix Services • 35
Client-Based vs. Clientless • 30
Communication Between an Internal Network and the Internet • 116
Communication Between Internal Networks • 116
Communication Examples • 115
Compliance Check • 37
Compliance Policy Rules • 37
Components of the Check Point Solution • 14

Configuring Alternate CRL Distribution Points • 131
Configuring Anti-Spoofing • 24
Configuring CGNAT • 144
Configuring Citrix Services for Mobile Access • 36
Configuring Compliance Settings for a Security Gateway • 39
Configuring CoreXL • 99
Configuring Fail Open When CRL is Unavailable • 132
Configuring Fragmentation for IPSec Traffic • 130
Configuring Gateways to Send Logs to Syslog Servers • 143
Configuring Geo Protections • 78
Configuring GSN Handover Group Limits • 136
Configuring GTPv2 Support • 133
Configuring HTTPS Inspection Rules • 72
Configuring IP Pool NAT • 122
Configuring New GTPv2 Message Types and Information Elements • 148
Configuring Persistent VPN Kernel Parameters • 132
Configuring Remote Access to Network Resources • 30
Configuring SCTP Acceleration • 136
Configuring SCTP Inspection • 134
Configuring SCTP NAT • 136
Configuring SecureXL • 100
Configuring Security Gateways • 71
Configuring Stateful NAT64 • 145
Configuring Static and Hide NAT • 107
Configuring Subnet Range Selection for Quick Mode IDs • 131
Configuring the GTP Signaling Rate Limit • 133
Configuring the Hit Count Display • 27
Configuring the NAT Policy • 102
Configuring the Security Gateway Object • 119
Configuring the Security Management Server Object • 119
Connecting to a Citrix Server • 35
Connecting Translated Objects on Different Interfaces • 114
CoreXL • 11, 98
Creating a Compliance Policy • 38
Creating a New AD Object • 53
Creating a Secure Firewall Rule Base • 21
Creating a Strong Firewall Security Policy • 19
Creating an Account Unit • 56
Creating Diameter Application Commands • 141
Creating Diameter Applications • 140
Creating Diameter SCTP Services • 138
Creating Diameter TCP Services • 139
Creating Reports • 125
Creating VPN Policies • 42
CSCF • 11
Using Hide NAT • 103
Using Identity Awareness • 50
Using Identity Awareness in the Firewall Rule Base • 54
Using IPS Profiles • 75
Using Remote Access VPN • 48
Using Secure Workspace • 40
Using SecureXL • 99
Using Site to Site VPN • 46
Using SmartEvent • 97
Using SmartView Tracker • 94
Using the Firewall Rule Base • 19
Using the HTTPS Inspection Rule Base • 69
Using the Identity Awareness Wizard • 51
Using the Mobile Access Configuration Wizard • 32
Using the URL Filtering and Application Control Rule Base • 64
Using User Directory • 55
UTMS • 13

V

Verification • 144
VPN Communities • 43
VPN Connectivity Modes • 48

W

Working with Access Roles • 53