



the CENTER for
INTERNET SECURITY

Check Point Firewall Benchmark v1.0

Editor: John Traenkenschuh

December 2007

Copyright 2001-2007, The Center for Internet Security (CIS)

<http://cisecurity.org>
cis-feedback@cisecurity.org

TERMS OF USE AGREEMENT

Background.

The Center for Internet Security ("CIS") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("Products") as a public service to Internet users worldwide. Recommendations contained in the Products ("Recommendations") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No Representations, Warranties, or Covenants.

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties, or covenants of any kind.

User Agreements.

By using the Products and/or the Recommendations, I and/or my organization ("We") agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and
6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even

if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;
2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of Intellectual Property Rights; Limitations on Distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled “Grant of limited rights.”

Subject to the paragraph entitled “Special Rules” (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations (“**CIS Parties**”) harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive

defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special Rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (<http://nsa2.www.conxion.com/cisco/notice.htm>).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

Terms of Use Agreement Version 2.1 - 02/20/04

Table of Contents

1	Provisos and Assumptions	6
1.1	Firewall Illustrations	6
1.2	Firewall Role and Setting	6
1.3	Firewall Platform	6
1.4	Administrator Requirements	6
1.5	Security Limitations	6
2	Securing the Base Installation	7
2.1	Place all Check Point equipment in a Secure Physical Setting	7
2.2	Apply latest OS patches	7
2.3	Create Secure Configurations for all Firewall Components	9
2.4	Change all default account IDs and passwords	9
2.5	Ensure Safe Source Practices for all Components Loaded Over the network	9
2.6	Install and configure Encrypted Connections to devices	10
2.7	Create and Use Certificate-based or Two-Factor Authentication	12
2.8	Record Logs without Resolving IP Addresses or Service Port/Protocol Numbers	13
2.9	Authorize Administrator GUIs by IP Address	14
2.10	Verify the Default Boot Process	15
2.11	Install and Run Network Time Protocol (NTP)	15
2.12	Enable Secure Logging	16
2.13	Secure SNMP	19
3	Implement Secure Default Settings	19
3.1	Enable the Firewall Stealth Rule	19
3.2	Configure a Default Drop/Cleanup Rule	19
3.3	Use Check Point Sections and Section Titles	20
3.4	Enable SmartDefense, in Monitor Mode When Possible	20
3.5	Review and Log Implied Rules	22
3.6	Create Anti-Spoofing Rules	22
3.7	Control ICMP	24
3.8	Inspect Inbound and outbound traffic	25
3.9	Ensure Periodic Version Control and Export of SmartCenter Configurations	25
3.10	Control Multicast and Broadcast Addresses	27
4	Appendix:	29
4.1	Changes Table	29
4.2	Sources	29

1 Provisos and Assumptions

1.1 Firewall Illustrations

All illustrations come from SmartConsole, running in 'demo' mode. No production rules or actual organization's firewalls provided the illustrations.

1.2 Firewall Role and Setting

This benchmark will document reasonable best practices for a Check Point firewall that is Internet facing and may selectively provide access to a DMZ setting. The benchmark does not discuss the use of firewalls for virus inspections of incoming traffic (Content-Vectoring Protocol) nor does it discuss the use of inbound or outbound web, ftp, rlogin, etc proxying services Check Point firewalls can provide.

1.3 Firewall Platform

The platform for this document is SecurePlatform, as provided by Check Point, using Check Point NGX/R65. Later documents may discuss Checkpoint running on Nokia platforms, running on Windows, Solaris, etc.

1.4 Administrator Requirements

This document assumes that implementers of this benchmark have received and passed appropriate Check Point training. Additionally, implementers should understand TCP/IP networks, principles of routing and switching, etc. This benchmark is no substitute for required training and experiences. It will not provide details on creating rules, multiple authentication technologies, etc.

1.5 Security Limitations

A Check Point firewall is only one small part of your organization's overall security architecture. While configuring the firewall, it is important to remember these key limitations:

- Firewalls cannot prevent hacks, once security decision makers allow vulnerable protocols, designs, and services. For example, once access to the CIFS share is given, firewalls cannot deny access to subdirectories below the root of the share. In this and other cases, organizations must apply proper Operating System security.
- Check Point Firewalls can provide limited inspection of application traffic, if organizations purchase add-on toolsets (such as Smart Defense). Even then, poor application security practices can severely undermine the security a firewall may provide.
- Although a Check Point firewall can inspect many types of Internet Protocol traffic, there are limitations:
 - Check Point cannot inspect encapsulated non-IP packets (NetBIOS over TCP/IP, SNA over IP, etc).

- Check Point cannot inspect encrypted traffic without organizations creating a design that ends the encryption, before passing the traffic through the firewall.
- Check Point cannot inspect non-IP traffic (AppleTalk, NetBIOS, etc).

2 Securing the Base Installation

2.1 Place all Check Point equipment in a Secure Physical Setting

Action:

Place all Check Point equipment in a setting secured from the public. Consider the possible impact of keeping floppy drives or USD drive ports enabled on the equipment.

Discussion:

People with physical access to a device can seize control of the device. Floppy drives (or their modern USB counterparts) can be used to reboot the device and either alter settings and binaries or to reload components over the network, from a compromised server. The Check Point equipment is some of the most important security equipment on the network, and thus, deserves adequate physical security.

2.2 Apply latest OS patches

Action (Secure Platform):

Download and install upgrades and patches from Check Point's website, currently at <http://www.checkpoint.com/downloads/index.html>. Follow the installation instructions.

Action (older Check Point releases):

Strongly consider upgrading to current releases.

Discussion:

Installing up-to-date vendor patches and developing a procedure for keeping up with vendor patches is critical for the security and reliability of the system. Organizations must patch each installed component of the Check Point Firewalling system. Vendors will issue operating system updates when they become aware of security vulnerabilities and other serious functionality issues, but it is up to their customers to actually download and install these patches.

Note: Several applications feature convenient interfaces to download updates within SmartDashboard, as shown in Figure 1. Similar interfaces are available for Content Inspection and SmartDefense Services, once their tabs are clicked. Finally, SmartUpdate itself features an easy interface to check for updates.

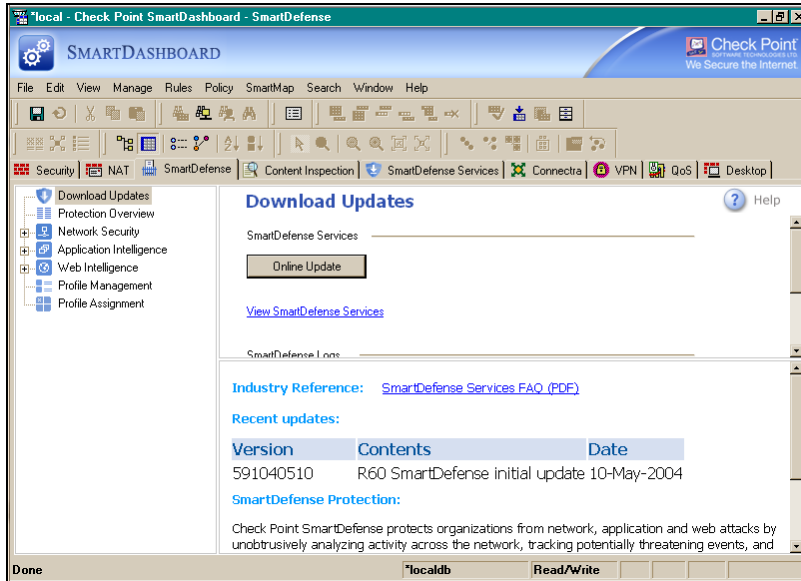


Figure 1a: Convenient Interface to Updating SmartDefense

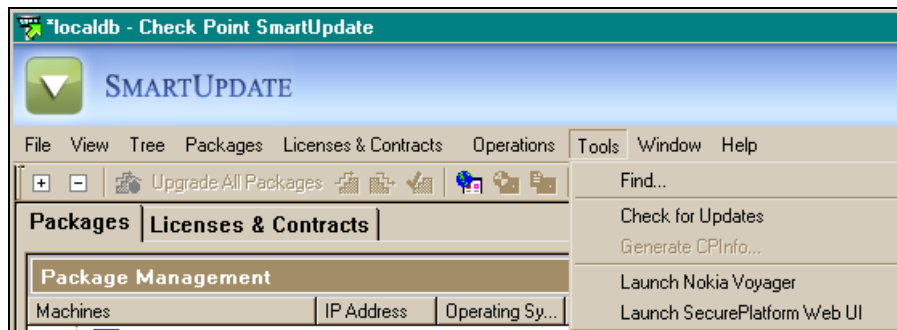
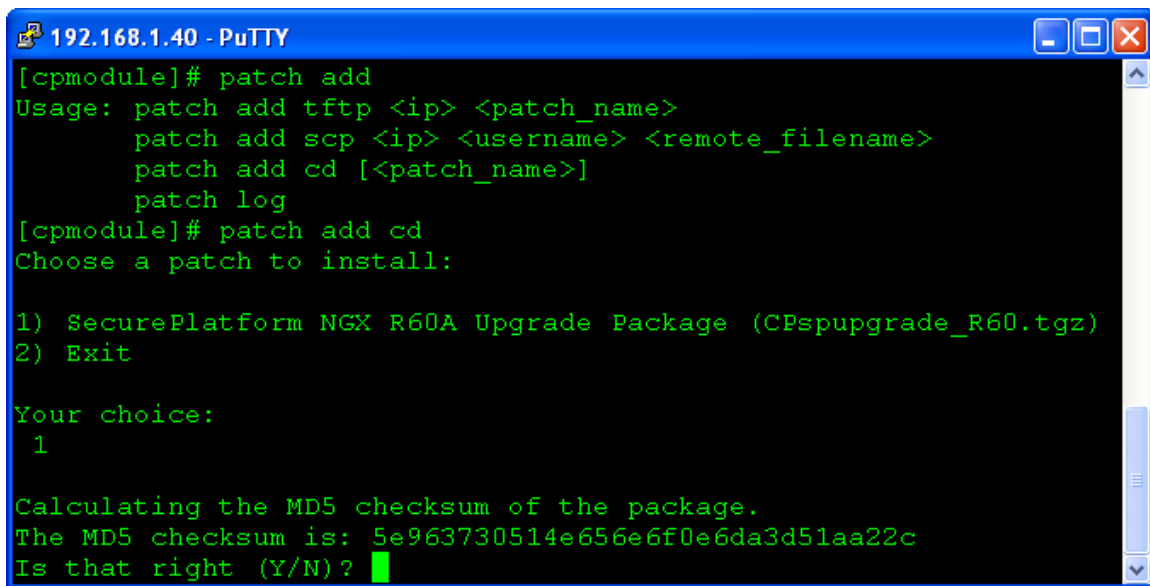


Figure 1b: Using SmartUpdate to check for Updates.

For Secure Platform systems, command line patches can be applied using the “patch add” command. Access the Secure Platform command line via SSH or local console, and then execute the “patch add” command at the prompt. Patches can be installed from CD or retrieved from remote systems using TFTP or SCP. When using the remote retrieval method, SCP is strongly recommended to secure the communication channel. All patches should be verified for MD5 integrity. Figure 1c demonstrates the “patch add” command, with a selection to patch from CD:



```
192.168.1.40 - PuTTY
[cpmodule]# patch add
Usage: patch add tftp <ip> <patch_name>
       patch add scp <ip> <username> <remote_filename>
       patch add cd [<patch_name>]
       patch log
[cpmodule]# patch add cd
Choose a patch to install:

1) SecurePlatform NGX R60A Upgrade Package (CPspupgrade_R60.tgz)
2) Exit

Your choice:
 1

Calculating the MD5 checksum of the package.
The MD5 checksum is: 5e963730514e656e6f0e6da3d51aa22c
Is that right (Y/N)? █
```

Figure 1c: SecurePlatform Patching from the Command Line

2.3 Create Secure Configurations for all Firewall Components

Action:

In addition to the firewall(s), organizations must configure the management servers and Administrator workstations securely. Organizations should start this process by following the CIS Benchmarks for these platforms, including the installation and use of anti-virus and anti-spyware software.

2.4 Change all default account IDs and passwords

Action:

Organizations must change the default passwords used during the installation of Check Point products, when prompted.

Discussion:

During the installation of several Check Point products, a default ID and password are used. Using admin/admin as your SmartCenter or SecurePlatform production management account and password is not recommended.

2.5 Ensure Safe Source Practices for all Components Loaded Over the network

Action:

If your Check Point device configuration loads components over the network, use products like Trip Wire to ensure that no one alters components with planted backdoors or Trojan code before any system loads.

Alternately, load devices on a private net not attached to the corporate network, and then move the new devices onto the rack. This is especially true for any exported configuration files that will be imported onto new equipment via TFTP. TFTP has no authentication mechanism, making it possible for an intruder to get a second copy of any firewall configuration file exported to the server. When possible, employ Secure Copy (SCP) or other secure data transfer methods.

Discussion:

New devices can be loaded over the network via FTP, HTTP, or NFS. FTP, Web technologies, and NFS have various security problems. Large organizations setting up a large Check Point installation may find a hacker has altered the source files to put backdoors and other problems into production.

Unfortunately, while the three loading technologies can offer a password, password use is not enforced. None of the three techniques will authenticate the identity of the safe source server, possibly allowing a server with hacked binaries to take the server's place.

2.6 Install and configure Encrypted Connections to devices

Action:

1. Ensure that SSH is running and logging on SecurePlatform. Ensure that no plaintext protocols (telnet, ftp, etc) are configured and running on the management server. SSH is an acceptable substitute for UNIX/Linux platforms.
2. If Windows is used, Remote Desktop Protocol/Terminal Services can be used to provide remote execution and file transfer abilities over an encrypted connection.
3. Configure Client Authentication, if used, to use an encrypted connection and instruct users to use a browser only.
4. Confirm plaintext protocols are not used.

Discussion:

Never access Firewalls and management servers with plaintext protocols. In addition to exposing passwords to sniffers, plaintext protocols have a history of enabling session hijacking.

1. SecurePlatform:

OpenSSH is a popular free distribution of the standards-track SSH protocols, which allows secure encrypted network logins and file transfers. However, compiling OpenSSH is complicated by the fact that it is dependent upon several other freely available software libraries that must be built before OpenSSH itself can be compiled. In order to simplify the installation and update process, we make use of a pre-compiled version of OpenSSH, available from Check Point via the SecurePlatform installation and later patching processes.

CIS recommends that Version 2 of the SSH protocol be used.

2. Windows:

Windows users can use the freely available RDP client to connect to a properly configured Windows server. This will provide an encrypted connection.

3. Client Authentication

Client Authentication allows a user and device to authenticate to the firewall and inherit pre-configured firewall rules for a set amount of time. By default, these connections are unencrypted yet can travel over unsecured networks.

It is recommended that all Client Authentication connections be made using the HTTPS configuration. This both uniquely identifies the gateway and keeps the authentication credentials from being copied when going over the network.

Note: Changing the port used for Client Authentication requires changing parameters in the \$FWDIR/conf/fwauthd.conf file. Administrators must use great care when doing this, and administrators should review SmartDefense/AdminGuide. Once the administrators are familiar with all operations, including stopping the firewall,

- A. Review the ‘nickname’ of the targeted gateway: Open the VPN page of the Gateways Properties window and review the Certificates List, as shown in Figure 2.

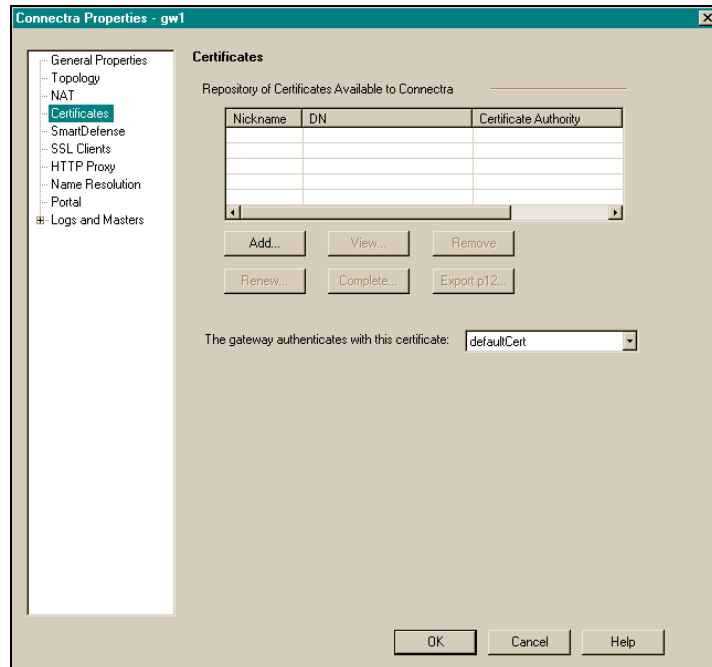


Figure 2: Reviewing the Certificates Available to a Gateway

- B. Locate the in.ahclientd line in the file. Move to the end of the line.
- C. Add the words, “ssl:defaultCert”, without using the quotation marks, if defaultCert is the certificate used by the gateway for authentication. Otherwise, put the name of the specific certificate used by the specific gateway implementing client authentication.

- D. This is an example of a completed line:
`'900 fwssd in.ahclientd wait 900 ssl:defaultCert'`. Be careful to avoid other changes.
- E. Save and close the file.
- F. Restart the firewall.
- G. Create a policy that allows users to use https and Client Auth with the Gateway.
- H. To disable the telnet service listening on port 259 by default, write a rule that prevents connections to the daemon in the rulebase.
4. Confirm that there are no plaintext ports listening.

Use a port scanner such as NMAP to see what ports are open and which services are responding from the firewall and related management devices.

2.7 Create and Use Certificate-based or Two-Factor Authentication

Action:

After the first login, the administrator can create a certificate for subsequent logins. Additionally, working with other administrators, new administrator certificates should be generated. The new Administrator should simply type in the password while creating the User object. Create and use a certificate for authentications to the SmartConsole. For additional information on how to create a certificate, refer to the SmartCenter Administration Guide. Figure 3 shows the User object button used.

Discussion:

Logging to the SmartCenter to do Administrative work requires more than a password for optimal security. This document advises Administrators to implement TACACS+, SecurID, or RADIUS server implementations to secure accessing the SmartCenter. If these designs are unacceptable to an organization, using certificate-based authentication is better than a static password going over the wire.

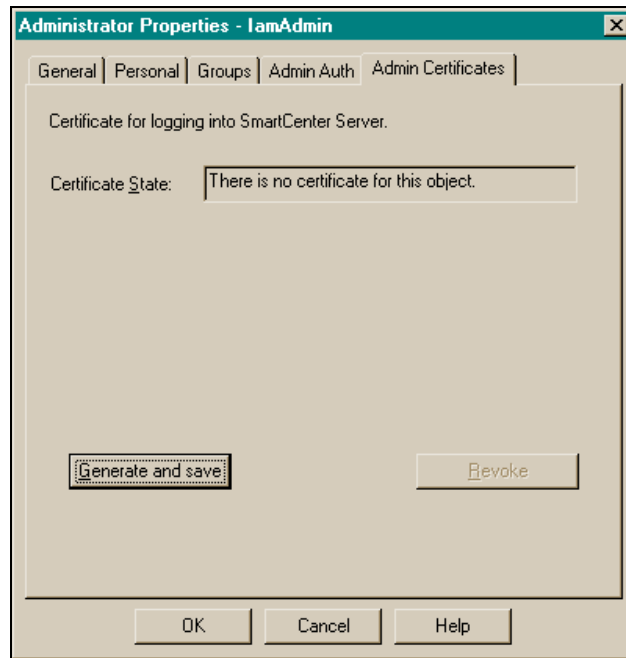


Figure 3: Generating a Certificate for a New Administrator

The certificate must be kept secure, and should have a strong passphrase applied to it. Additionally, the computer housing it needs anti-virus and patching, etc.

2.8 Record Logs without Resolving IP Addresses or Service Port/Protocol Numbers

Many events happen each second. The time spent resolving Addresses or Port/Protocol numbers can add delay to a busy firewall. Additionally, this can provide another attack vector for intruders who attack DNS, local Services files, etc. If the information is needed, consider use of tools that can resolve IP addresses as part of a log export and secure storage process. JDResolve is one such application.

To disable resolution, untoggle the selections in the SmartTracker main menu, as shown in Figure 4.

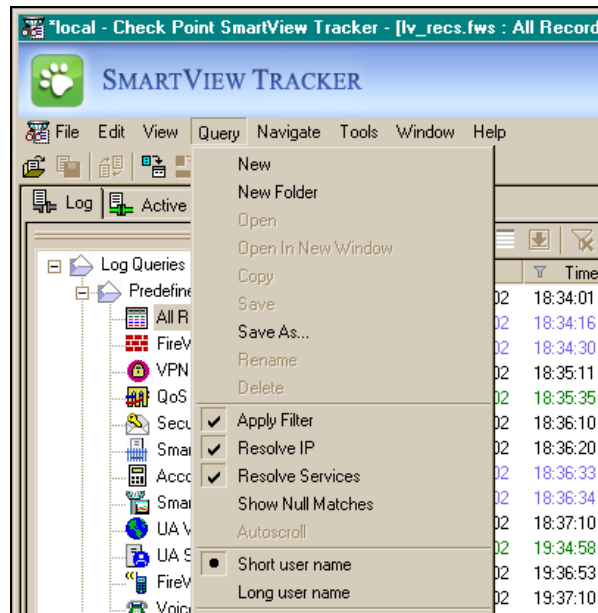


Figure 4: Removing Resolution Options

2.9 Authorize Administrator GUIs by IP Address

Action:

A GUI Client are identified by either IP address or Name (if the Name is routable on the network). Choose to identify the client by IP address.

Discussion:

Names, whether IP hostnames or Windows NetBIOS names, are a level of abstraction that can have security or performance issues. If DNS cache is poisoned, for example, another GUI, one attempting to open the firewall, may steal the hostname. NetBIOS names given by WINS or LMHOSTS or other means can be counterfeited with little impact to the network. IP addresses are much more difficult to falsify, although, admittedly, ARP tables can be corrupted. Among the three choices, IP addresses are the most difficult device identifier to counterfeit. This said, choosing IP address means that the Administrator must be careful to get a static or long lease DHCP assignment for the computer hosting the GUI.

There are two administrative interfaces: SmartCenter and the SmartPortal, itself a web Interface to the SmartCenter. Limiting the IP address is best done in both interfaces.

To limit GUI client access to the SmartCenter , run cpconfig. Define GUI clients or the term 'GUI Clients' is the section that allows each IP address for authorized clients to be defined. IP Addresses can be defined by IP/Subnetmask, by wildcarding network parts, by IP Ranges, etc.

For a firewall gateway running SecurePlatform and the web interface, administrators can access the Device -> Web and SSH Clients and configure the IP addresses/subnet masks there, to limit access to the web interface/ssh access as well.

SmartPortal will require editing/creating a configuration file in the SmartPortal conf directory.

1. Stop the SmartPortal services.
2. Navigate to the conf directory.
(Windows: C:\Program Files\CheckPoint\R65\SmartPortal\portal\conf *NIX and SmartPlatform: /opt/CPportal-R65/portal/conf .)
3. Open (or create) the hosts.allow file with a plaintext editor.
4. Create an entry for each Administrator that begins with the services allowed and the specific IP addresses (or summarized addresses) able to use the services: ALL: 1.2.3.4/255.255.255.0 . This example allows the administrator at 1.2.3.4 to access SmartPortal services.
5. Start the SmartPortal services.

2.10 Verify the Default Boot Process

Action:

Occasionally verify that the gateway loads the Default Filter and Initial Policy. Alternately, do NOT alter the default Policy without ensuring all repercussions are known. Document the changes and share them with all other administrators. To verify loading of the Default Filter or Initial Policy:

1. Boot the system.
2. Before installing another security policy, type the following command:

```
$FWDIR/bin/fw stat
```

The command's output should show that defaultfilter is installed for the Default Filter status. It should show that InitialPolicy is installed for the Initial Policy.

Discussion:

Networks are open to attack during the time the gateway reboots and the policy ruleset is loaded. In normal operation, IP forwarding is disabled and the gateway takes very few connections. It is important to verify that this critical security process has not been disabled or changed by accident or by malicious intent.

2.11 Install and Run Network Time Protocol (NTP)

Action:

Ensure NTP or an acceptable substitute is providing accurate time sourcing to the management server and all gateways. Acceptable substitutes may be the time sourcing services the management server may get from the domain, if the domain is using NTP.

Discussion:

Logs are vital to security. Equally vital are accurate log events. Step one is to ensure devices participating in logging (i.e., sending events to the logging server or recording the events) have an accurate time source. Additionally consider recording log in GMT format, a format that does not interject confusing time anomalies, like Daylight's Savings Time changes, into the logs.

NTP can be confirmed quickly by running a port scanner to see if the system is listening for NTP traffic, on port 123.

Configuring NTP on SmartPlatform:

1. At the command line prompt, type:
`ntp -n 600 {IP address of the NTP Server}`

Notes:

- 600 indicates the interval for polling for new time values. Use a value recommended by your organization.
- Your organization may have an NTP architecture, in which case, you may use the IP address of an internal NTP server
- You should have multiple NTP servers in your NTP design
- You can use IP addresses or Hostnames of NTP servers. Using IP address brings no DNS dependencies. Using Hostnames insulates your settings from IP address changes. You may want to use a mix of IP addresses and hostnames to ensure highly available NTP services.
- Ensure that the firewall devices contacting NTP servers have rules allowing this in the rulebase, including the firewall itself.

2.12 Enable Secure Logging

Action:

Review SmartCenter Logging abilities and select those that are appropriate for your organization. This document specifically recommends logging failed authentications. Using native syslog abilities (UDP 514) has several security issues.

Discussion:

Determining what events to log is dependent on many factors, the amount of disk space for short-and long-term log retention, an organization's ability to scan and react to bad events in logs, etc. Hackers will attempt to take control of a firewall if the rulebase cannot be bypassed, so logging and scanning for failed authentication attempts is valuable.

Native syslog is UDP-based and is open to packet interjection attacks. Any receiving logging server can be open to Denial-of-Service attacks by attempting to flood the logging Daemon.

Check Point has a centralized logging server that can be installed with the management server. Administrators can configure Check Point gateways to have their logs sent to the management server, using encrypted and authenticated channels. To do so with your installation:

1. Retrieve the activation key applied during the setup and configuration of the management server.
2. Open SmartDashboard. Open the 'Network Objects' pane and right-click on Check Point, to select 'New Check Point' to create the gateway.

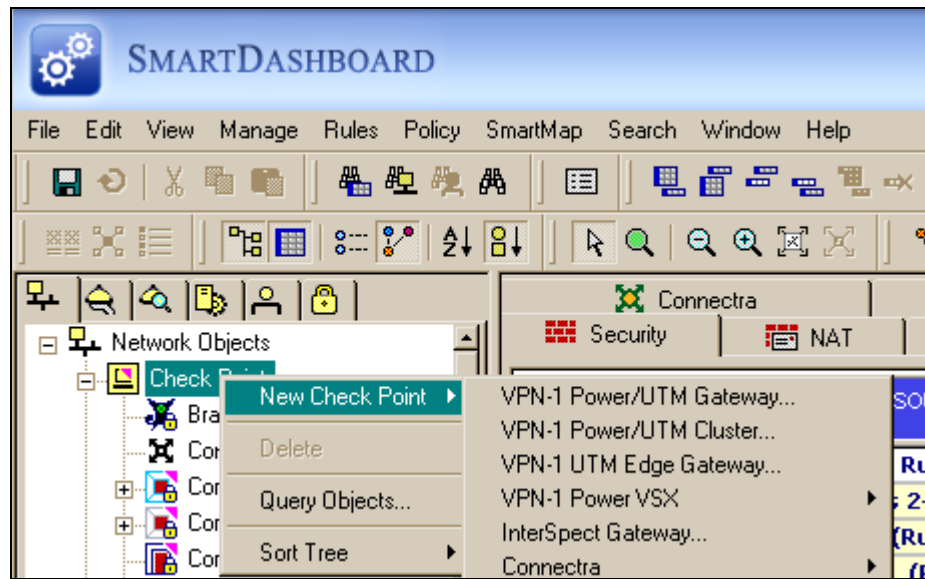


Figure 5: Creating A Gateway

3. At the 'Check Point installed Gateway creation' dialog box, select 'Classic mode'.
NOTE: This dialog box only appears if the reader (or another administrator) has not already set a preference for Classic versus Wizard mode.
4. In the General Properties pane item, fill in the name, address, etc of the installed gateway.
5. The encrypted channel (SIC) must be initialized with the activation key. To do so, click the Communication box.
6. Input the activation key and click the initialize button, as shown in Figure 6. (If the correct code is used, the Trust State window will change to 'Trust Established'.)

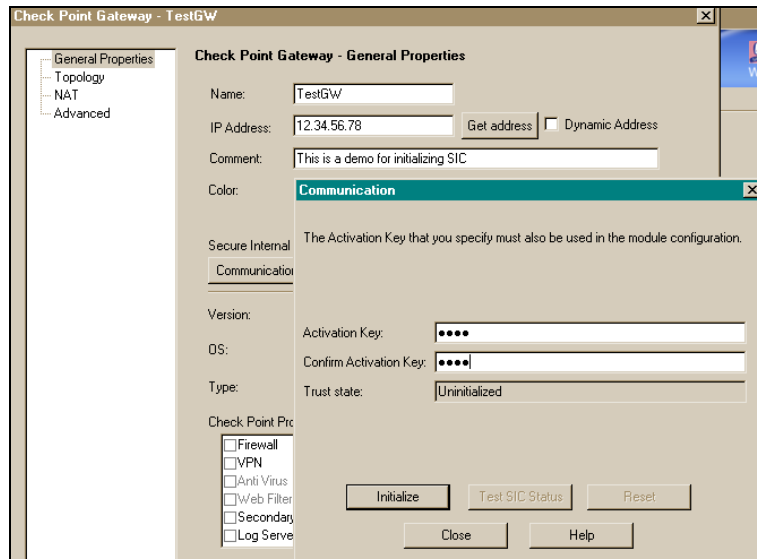


Figure 6: Initializing SIC Communications

Now that the Gateway is capable of communicating with the SmartCenter server via an encrypted channel, it is time to set the Gateway's logging abilities to use the SmartCenter server.

1. Open the Gateway object by finding it in the Network Objects tab in the SmartDashboard tool. It will be listed in the 'Check Point' subsection.
2. Select the plus symbol next to 'Logs and Servers' to open it. Select 'Log Servers' to configure which server will be used.
3. Simpler architectures can select 'Use local definitions for Log Servers' to select the default logging server. Complex architectures with multiple SmartCenter servers can choose 'Define Log Servers' to select the desired logging server. Click the 'Add' button to see and to select the desired logging server.
4. Figure 7 shows the Management server being selected. Click Ok in all dialogs to save the configuration. If you have not selected a Master previous to this step, you will be asked to do so as you close the panels.

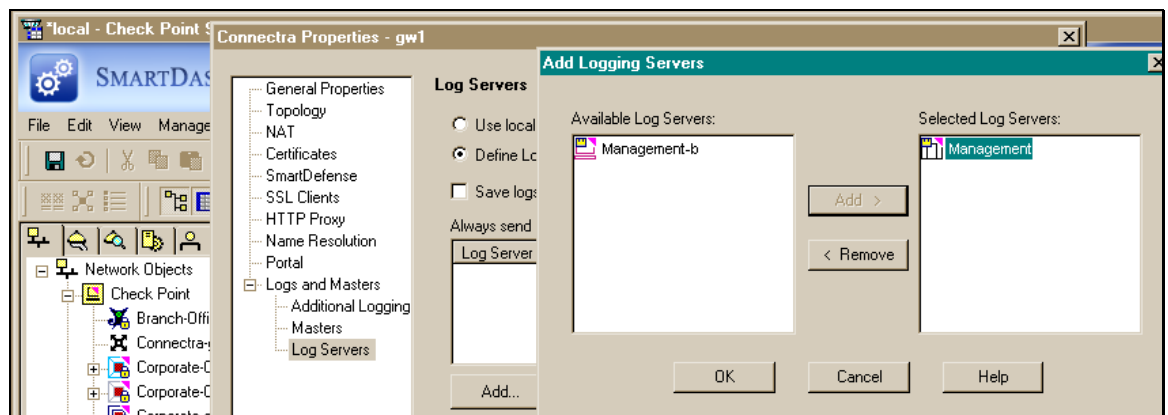


Figure 7: Adding and Selecting a Logging Server

2.13 Secure SNMP

Action:

If SNMP v1 must be used, ensure that all community strings are set to unpredictable values. Common defaults include 'Public' and 'Private', and it is recommended that these values not be used.

Discussion:

Tools such as SNMPWalk can reveal active SNMP MIBs on the equipment and attempt known defaults such as public or private. To configure the community string in SecurePlatform:

1. SNMP settings are stored in /etc/snmp/snmp.conf.
2. Open the file for editing. You may need to stop the firewall service if working on the firewall.
3. Search for the trapcommunity directive
4. Edit the string following the directive trapcommunity to be an unpredictable, non-default value.
5. Save the file.
6. Restart all stopped services.

3 Implement Secure Default Settings

3.1 Enable the Firewall Stealth Rule

Action:

Create a rule to drop Any Service from Any Source or Any VPN that attempts to connect to the gateway.

Discussion:

The stealth rule will limit access to the gateway to the control and service connections enabled as part of the design. As such, it is very important to enable access to the gateway as its role changes, for example, become a client VPN gateway. Another common example is enabling Client Authentication. If ports TCP 259 and 900 are not opened (or if you change the ports in the conf file), access will not work. Organizations with many Check Point gateways may want to document each gateway and the Check Point services it is intended and configured to accept.

3.2 Configure a Default Drop/Cleanup Rule

Action:

Ensure that the final rule in the rulebase explicitly drops all services, destinations, etc not specifically allowed in the previous rules.

Discussion:

It is important that any access not explicitly allowed be explicitly dropped. Figure 5 illustrates a typical rule. Administrators are reminded to check the specifics of their own network designs.



Figure 8: Typical Cleanup Rule

3.3 Use Check Point Sections and Section Titles

Action:

Use Sections to organize rules into related groups, whenever possible. Set each off with a descriptive Section Title.

Discussion:

Rulebase clarity helps all workers and reviewers. By organizing rules, inserting new rules is easier, and all can see the relationships among rules.

3.4 Enable SmartDefense, in Monitor Mode When Possible

Action:

Enable SmartDefense and evaluate its use in Monitor Mode.

Discussion:

SmartDefense is an excellent way to scan incoming traffic for possible attacks. Legacy Check Point logic to reassemble fragmented packets, inspect and drop IP Source Routed Packets, and stop Denial of Service attacks through spurious connections is in SmartDefense. Consider enabling 'Network Security' checks as a baseline.

We suggest monitor mode to see if Preventative mode will break production applications. In some cases, applications may count on unpatched configurations or may place odd bytes into headers, simulating actual attack traffic. In these cases, it is best to monitor and work to debug applications before enabling automatic prevention modes.

Administrators are cautioned to enable checks in measured 'waves'. Each check will add to the system load, in some cases dramatically. We believe strongly that the Network Security checks are called for, especially when facing the Internet, and recommend hardware upgrades if performance suffers appreciably as checks are enabled.

Figure 9 illustrates how to activate and log Network Security precautions; those we feel are most needed and beneficial. Administrators can activate or deactivate these checks—there is not monitor-only mode. We feel that logging the activity will show where the checks may be reacting to traffic in error. Alternately, a full range of responses is possible, including alerts and the like.

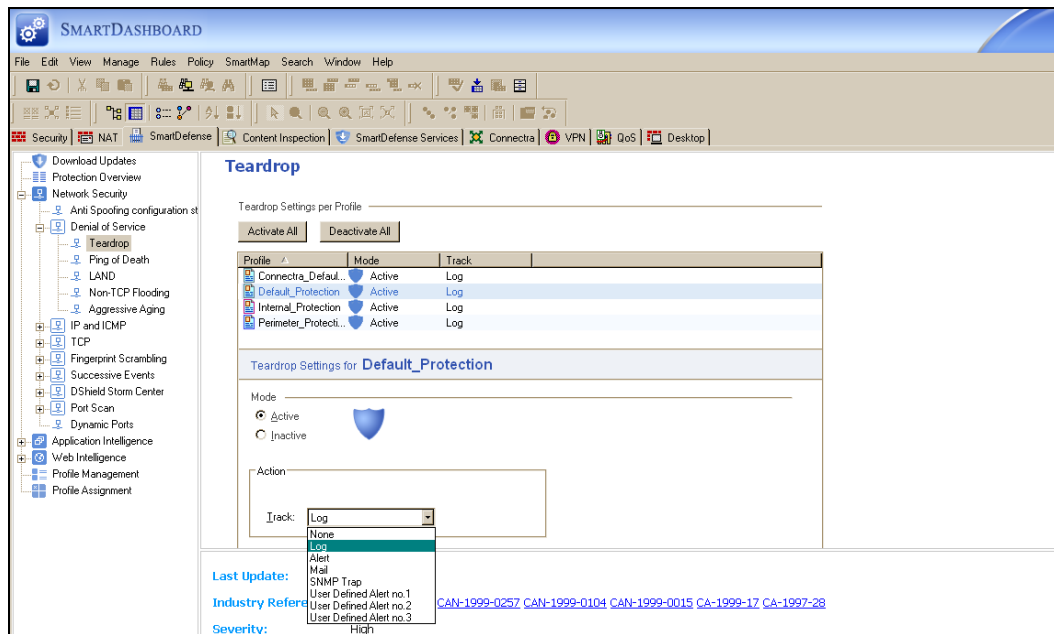


Figure 9: Enabling Network Security Checks and Logging

Figure 10 illustrates how to implement Application Intelligence checking into monitor mode, in this case, checking IMAP/POP3 connections for a wide variety of problems.

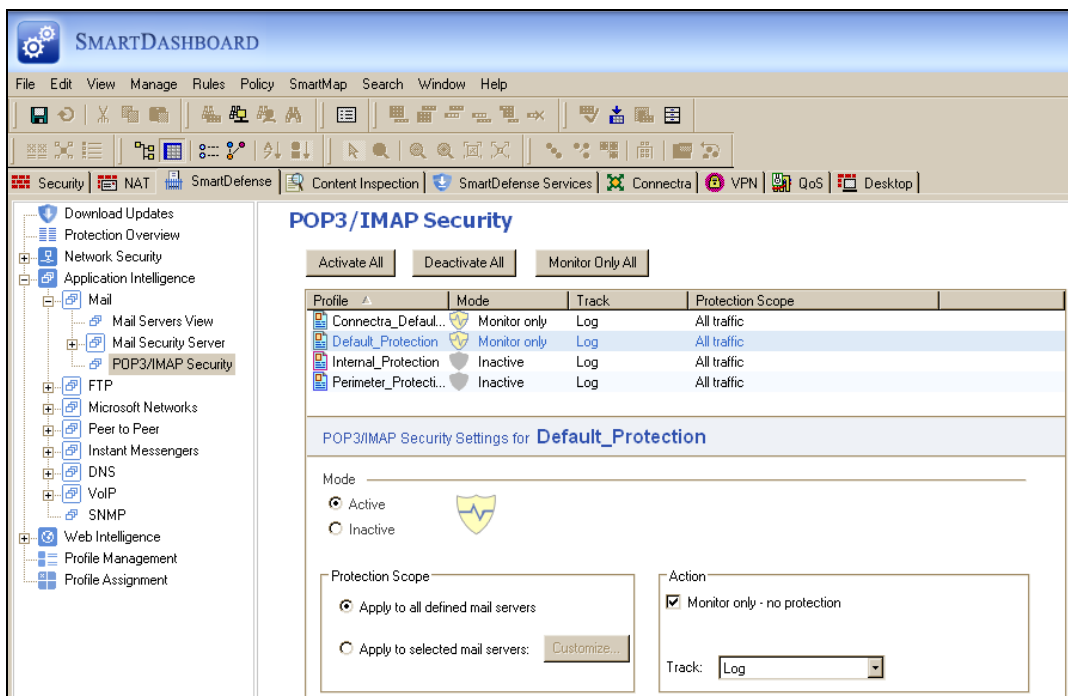


Figure 10: Enabling Application Intelligence in Monitor only Mode

3.5 Review and Log Implied Rules

Action:

It is recommended to define rules explicitly rather than state them implicitly in the Implied Rules section of Global Properties. If Implied Rules are used, configure logging for implied rules by accessing the 'Global Properties' dialog box, under the Policy menu. Figure 11 illustrates the checkbox, located at the bottom of the dialog box.

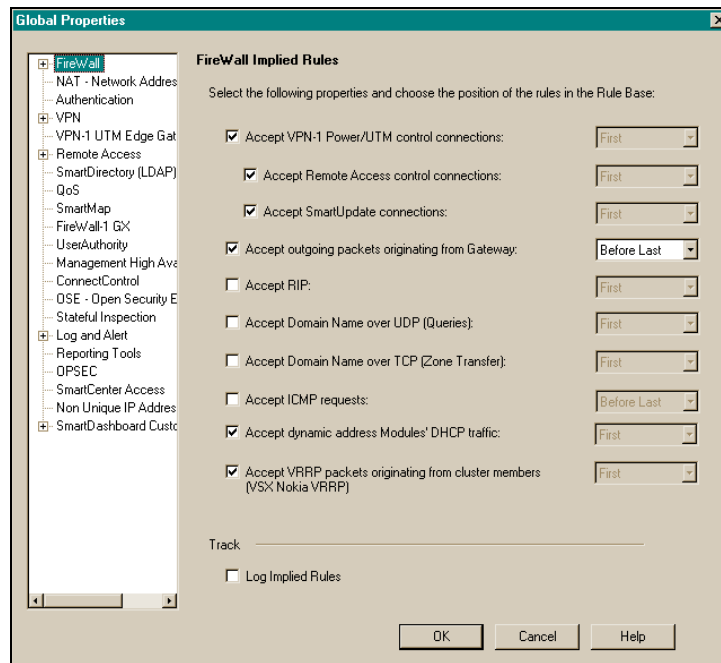


Figure 11: Selecting 'Log Implied Rules'

Discussion:

Rulebase clarity helps all workers and reviewers. Stating rules explicitly in the rulebase makes policy analysis and review significantly easier. Select the 'Log Implied Rules' to ensure all understand when connectivity is denied or allowed through a subtle Implied Rule.

3.6 Create Anti-Spoofing Rules

Action:

Ensure that explicit anti-spoofing rules are created to drop traffic from networks outlined in RFCs 1918 and 3330.

Discussion:

It is recommended that you specifically drop traffic from 10/8, 172.16/12, 192.168/24, etc that attempt to infiltrate your external interface. Less well known is RFC 3330. 169.254/16, for example, is often implemented for connection sharing, 'Link Local' services. In all cases of networks reserved by IANA, it is vital to ensure there is no logic

hole in your firewall design. Filter these addresses and your internal addresses from passing through the external interface. Check Point configures out-of-context addresses to filter automatically, once anti-spoofing is turned on.

Example: Applying anti-spoofing rules to the internal interface

1. Open the object of the gateway and select 'topology' in the left-hand pane. Double-click the internal interface, highlighted as eth1 in Figure 12.

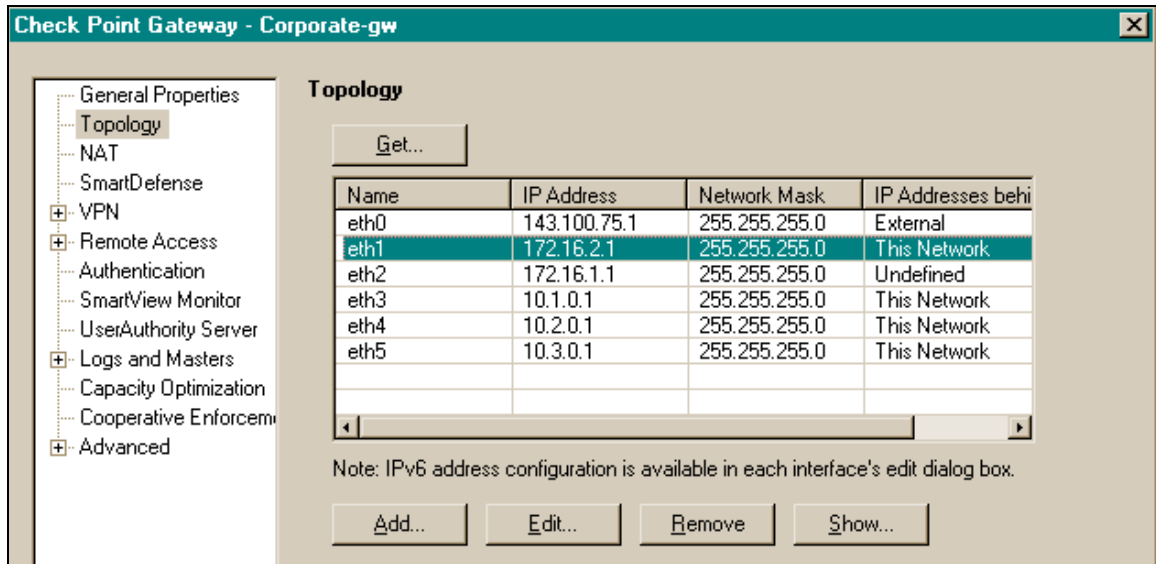


Figure 12: Selecting the internal interface

2. In the Interface Properties panel, ensure 'Perform Anti-Spoofing based on interface topology' checkbox is selected and select the response you wish to enable if an attack is detected, as shown in Figure 13.

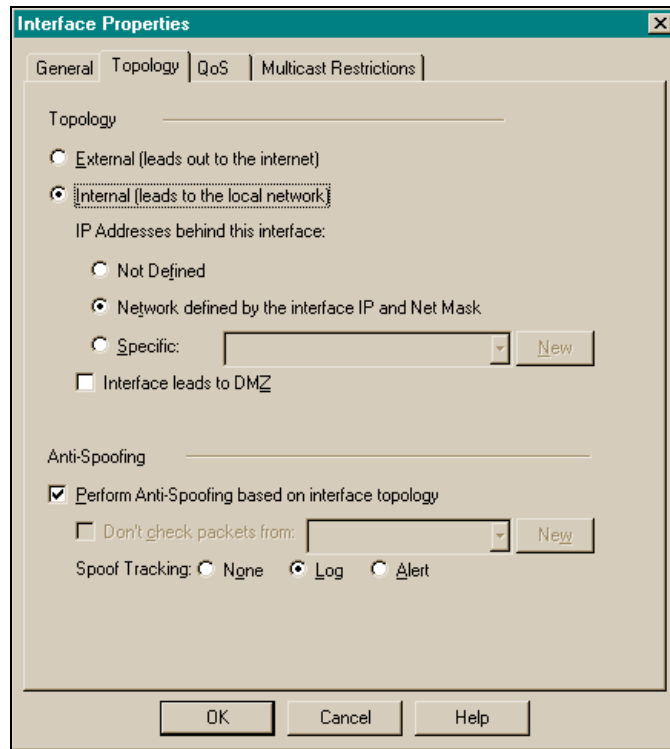


Figure 13: Enabling Anti-Spoofing

3. Close each panel by clicking the ok button. Perform the same steps on the external interface and all other internal interfaces.

3.7 Control ICMP

Action:

Specifically ban ICMP type 5, “Redirect”. Determine whether to drop inbound ping from the Internet. Determine whether to drop outbound ping to the Internet. Review

Discussion:

ICMP is a protocol used to control the network formation and ongoing operations. The redirect message can be sent to update a device’s gateway settings.

Ping is a useful network troubleshooting service. Attackers may use ICMP redirect messages to force traffic through a device running a sniffer, and thereby monitor traffic that layer 2 switches might try to isolate. Ping can be used in basic reconnaissance and with denial of service attacks.

While some organizations allow outbound ping, we believe it is better to block ping between the internet and the secure organization. Some viral worms have used ping as a means to find other hosts and networks to infect.

<http://www.cymru.com/Documents/icmp-messages.html> discusses ICMP messages and their [mis]uses. Your organization may decide to control messages beyond these recommended in this section.

3.8 *Inspect Inbound and outbound traffic*

Action:

Ensure that the firewall is in the default outbound route. Ensure that all incoming traffic passes through the firewall. Ensure that layer 2 edge devices forward through the firewall.

Discussion:

Attacks not only come into the organization; an attacker may use an organization's devices to attack the Internet. It is surprising how many organizations are careful to route inbound traffic through the firewall but neglect to ensure the firewall is the default outbound route. Additionally, it is saddening to see an edge router implement Proxy Arp and thereby by-pass the firewall.

In other cases, application developers take it upon themselves to dual-home a DMZ host, to ensure support from home. Some organizations implement separate VPN tools and gateways that become 'peers' to the firewall, even if the other technology has no firewalling, logging, inspection abilities.

Large organizations must partner to ensure that all traffic is inspected and that there are no alternate paths around the firewall.

3.9 *Ensure Periodic Version Control and Export of SmartCenter Configurations*

Action:

Backup key configurations done at both the system and security configuration levels.

1. Use Database Revision Control to create versions of the configuration at important events (adding new VPN domain, new gateway, etc.).
2. Periodically use 'Save As' to save and organize policy packages.
3. Regularly backup all SecurePlatform system configuration.
4. Create extensive SecurePlatform snapshots

Discussion:

In the same way that a lot of work goes into setting a Check Point Security Architecture, work must go into the organizing and saving of key stages of the work. Vast change can create a string of events that can create outages; in these cases, the right tools and procedures lessen downtime. This process begins with a plan and written procedures for managing change.

This section will describe technical operations that are important to the overall process. Each organization and implemented architecture can have varying needs. While we cannot give exacting details in a general security benchmark, all of us believe strongly in the maxim, “Save Early—Save Often”.

1. Create database versions at key change events.
 - a) Open SmartDashboard and under File, select Database Revision Control. Click the Create button to go on.
 - b) If necessary, you will be prompted to save the existing set of changes.
 - c) Input a general name for the set and a comment describing the reason for the save event.

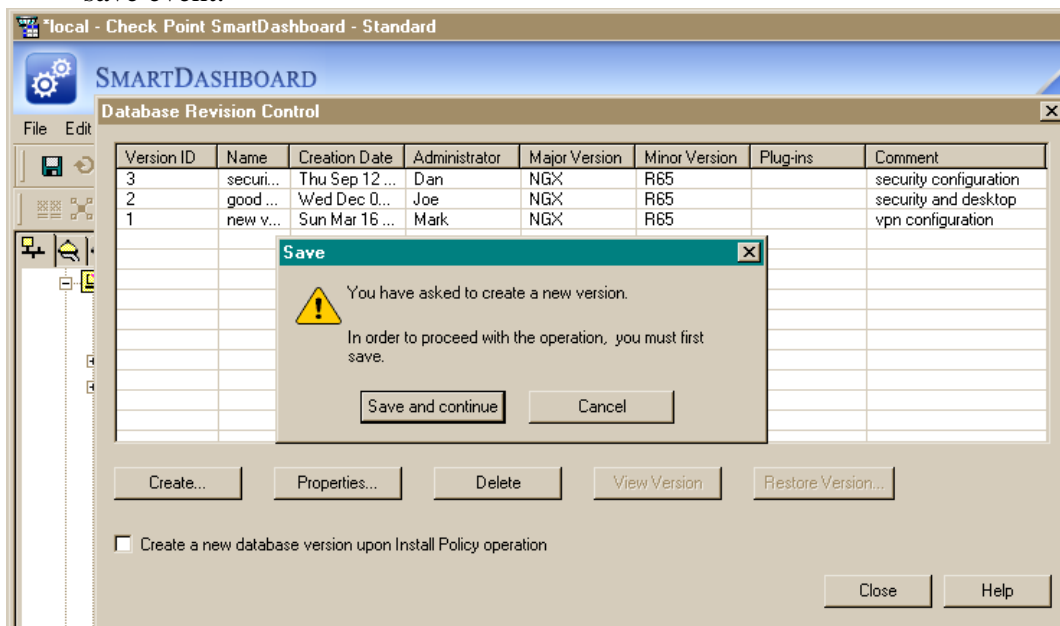
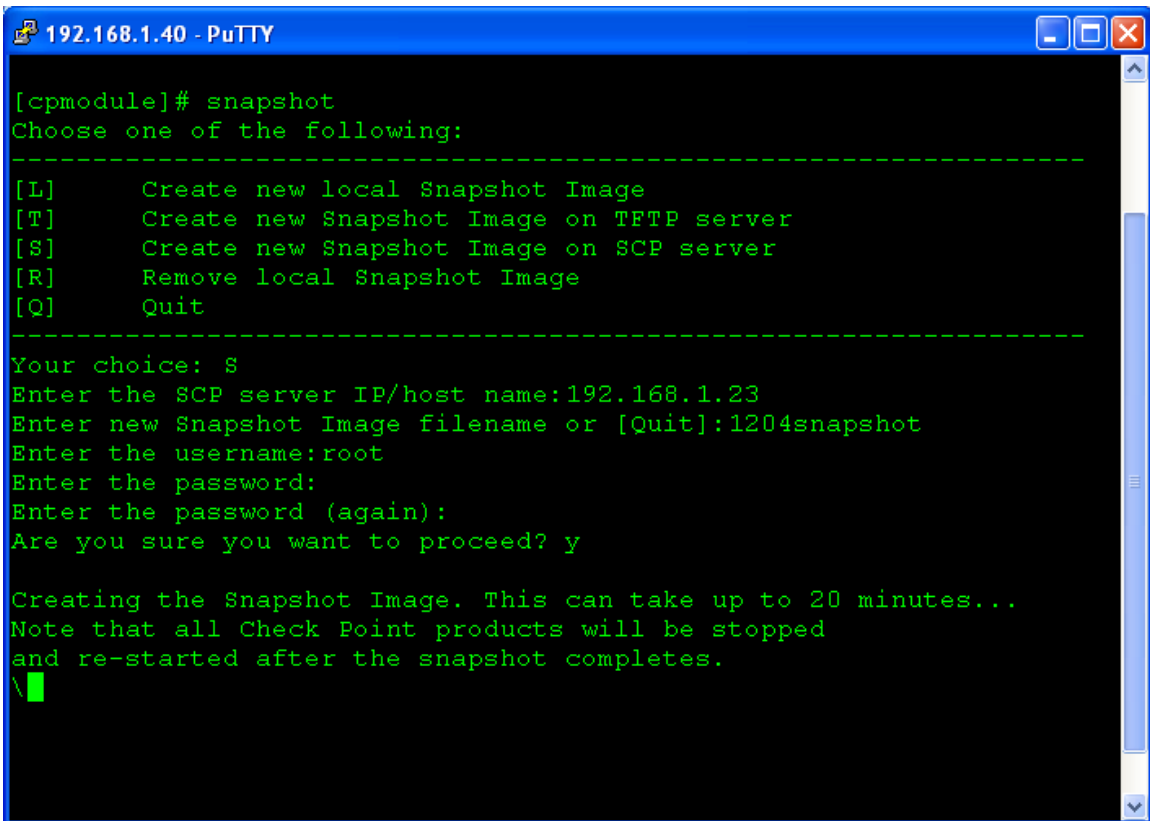


Figure 14: Creating a Database Version

2. Use ‘Save As’ to create a policy package
Open SmartDashboard and select ‘Save As’ to create a policy package—a collection of related policies. These packages allow administrators to build up policy modules that ensure appropriate polices are applied to each access control point. Give each package a descriptive name.
3. Backup SecurePlatform system configuration
There are many different options for backing up the system configuration. The simplistic command is `backup -file -path /tmp {MyBackupFilename}`. This command will create a backup file with the name of your choice in the /tmp directory.
4. Create extensive SecurePlatform snapshots
A snapshot records much more information than a mere backup (documented in step 3). By creating a snapshot, you create a comprehensive record of the system and system settings. This will create a large file. To create the snapshot, use the

command `snapshot -file -path /tmp {MySnapshotName}` . This makes a snapshot file (with a filename of your choosing) in the /tmp directory.

NOTE: Both the backup and snapshot commands support recording the files to a remote TFTP or SCP server. TFTP is a minimalistic file transfer server with no secure authentication design. SCP is a far more secure alternative, yet can be sensitive to network issues, especially with large file sizes. This CIS team recommends using an SCP server that is located close to the system(s).



```
192.168.1.40 - PuTTY
[cpmodule]# snapshot
Choose one of the following:
-----
[L]   Create new local Snapshot Image
[T]   Create new Snapshot Image on TFTP server
[S]   Create new Snapshot Image on SCP server
[R]   Remove local Snapshot Image
[Q]   Quit
-----
Your choice: S
Enter the SCP server IP/host name:192.168.1.23
Enter new Snapshot Image filename or [Quit]:1204snapshot
Enter the username:root
Enter the password:
Enter the password (again):
Are you sure you want to proceed? y

Creating the Snapshot Image. This can take up to 20 minutes...
Note that all Check Point products will be stopped
and re-started after the snapshot completes.
\█
```

Figure 15: The Snapshot Utility

3.10 Control Multicast and Broadcast Addresses

Action:

Determine if Multicast and Broadcast traffic should be allowed through the firewall, otherwise block it.

Discussion:

Multicast IP transmits a single message to a predefined group of recipients. An example of this is distributing real-time audio and video to a set of hosts that have joined a distributed conference.

When you enable multicast on a VPN-1 gateway running on SecurePlatform, you can define multicast access restrictions on each interface. These restrictions specify which

multicast groups (addresses or address ranges) to allow or to block. Enforcement is performed on outbound multicast datagrams.

Each IP network by default has a broadcast address that will reach all hosts on the network. In addition to the broadcast address for each subnet, there is a global broadcast address at 255.255.255.255.

Hackers will often pose attacks to the broadcast addresses, knowing that it will reach all nodes. If a computer with poor security is found, it will be used to attack a second, targeted computer, via any exploitable trust relationships among all computers on the subnet (Page 68, *Exploiting Software*).

Creating Broadcast and Multicast ‘Stealth’ rules ensures that these connections are not accessible by default.

Multicast Stealth rule parameters:

Src-Any, Dst-224/4, Svc-Any, Action-Drop, Track-Log

Broadcast Stealth rule parameters:

1. Calculate the broadcast address for the firewall interface. (Example: Network = 1.2.3.4/24 and broadcast address = 1.2.3.255).

2. Create the rule as follows:

Src-Any, Dst-1.2.3.255, 255.255.255.255, Svc-Any, Action-Drop, Track-Log

4 Appendix:

4.1 Changes Table

Version	Changes
0.1.0	Basic format and a little info
0.2.0	More information, more good controls found in Checkpoint Administrative PDF's <ul style="list-style-type: none">• Change default id/passwords• Network installation & import of config
0.3.0	Began Screen Captures and how-to. Added Administrator requirements (to ensure administrators get needed training from employers). Removed passive voice constructions. Removed individual call outs for appreciated help. Removed pictures. Added figures and illustrations. Core Team: Buena, Ryan; Kress, Chet; Morgan, Dai; Opatrny, Justin; Rodham, Dave; Shackelford, David; and Traenkenschuh, John, PM
0.3.3/3.5/3.6	Requested Edits/Logging, backup tactics

4.2 Sources

www.cymru.com/bogon

<http://www.cymru.com/Documents/icmp-messages.html>

Dowd, Mark, McDonald, John, and Schuh, Justin. *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*. Upper Saddle River, NJ: Addison-Wesley, 2007.

Hoglund, Greg and McGraw, Dr. Gary. *Exploiting Software: How to Break Code*. Boston: Pearson Education, Inc, 2004.

Goncalves, Marcus and Brown, Steven. *Check Point FireWall-1: Administration Guide*. New York: McGraw-Hill, 2000.

Lam, Kevin, LeBlanc, David, and Smith, Ben. *Assessing Network Security*. Redmond: Microsoft Press, 2004.

Northcutt, Stephen, Zeltser, Lenny, Winter, Scott, Frederick, Karen Kent, and Ritchey, Ronald W.. *Inside Network Perimeter Security*. Indianapolis: New Riders, 2003.

Ratcliffe, Andrew and Shah, Inti. *Check Point VPN-1/FireWall-1 NG Administration*. Emeryville, CA: McGraw-Hill/Osborne, 2003.

Smith, Ben and Komar, Brian. *Microsoft Windows Security Resource Kit*. Redmond: Microsoft Press, 2003.

Welch-Abernathy, Dameon D. *Essential Check Point FireWall-ING*. Boston: Addison-Wesley, 2004.

Zwicky, Elizabeth D., Cooper, Simon, and Chapman, D. Brent. *Building Internet Firewalls*. Sebastopol, CA: O Reilly, 2000.

Check Point Administrative PDF files also provide excellent documentation for firewall features and security configuration details.