GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Implied Rules in Checkpoint Firewall-1 NG AI

Mark Crowther

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b
Date Submitted: 13th July 2004

Abstract

Checkpoint Firewall-1 is an industry standard firewall product. The default installation of this firewall creates a number of rules in the firewall's rulebase that are, by default, hidden and are therefore often overlooked by the firewall administrator. These are known as 'Implied Rules'. This study will investigate the roles of implied rules in Checkpoint's Firewall-1 product (specifically Checkpoint Firewall-1 NG AI R54).
The report will begin with an overview of the Checkpoint Firewall-1 Infrastructure. Following this will be an explanation of implied rules, what they are, how and why they exist and best practice concerning their usage. The study will then go on to examine the implied rules in detail, the implications of the rule existing, and also how each rule should be handled. Finally the paper will explain how to disable and manually recreate the implied rules using SmartDashboard.

Checkpoint Firewall-1 Infrastructure Overview

Before discussing Checkpoint implied Rules it would be of use to understand the Checkpoint Firewall-1 infrastructure and how the components interact.

Firewall-1 is an industry standard firewall product made by Checkpoint. The Product can reside on the following Operating Systems. *(CHECKPOINT, 1)*

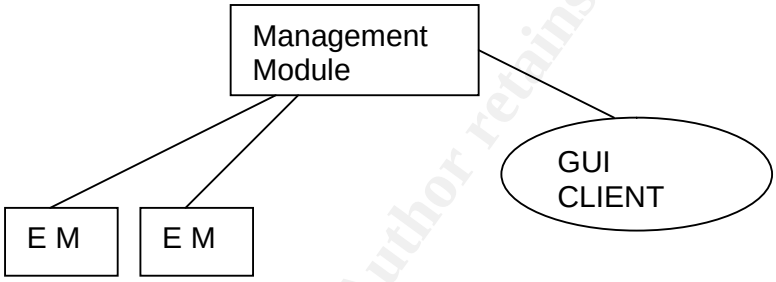
- Microsoft Windows NT 4.0 Server (SP6a).
- Microsoft Windows 2000 Advanced Server (SP1, SP2).
- Microsoft Windows 2000 Server (SP1, SP2, SP3).
- Solaris 8 UltraSPARC (32-Bit and 64-Bit).
- Solaris 9 UltraSPARC (64-Bit Only).
- Linux 7.0 (Kernels 2.2.16, 2.2.17, 2.2.19).
- Linux 7.2 (Kernels 2.4.9-31).
- Linux 7.3 (2.4.18-5).
- Checkpoint SecurePlatform NG with Application Intelligence.
- Nokia IPSO 3.7.
- AIX 5.2.
- "Secured By Checkpoint" Dedicated Security Appliances.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Firewall-1 enforces security policy at both the Network Level and the Application Level. The AI version of the software includes Application Intelligence, through which extra levels of protection can be employed. For example P2P communications (such as KaZaa) over HTTP can be denied even though HTTP communication is allowed.

Firewall-1 also tracks the state of each communication using Stateful inspection. In Stateful Inspection:
"Filtering decisions are based not only on administrator-defined rules (as in Static Packet Filtering) but also on context that has been established by prior packets that have passed through the firewall". *(WEBOPEDIA, 2)*

The Checkpoint Firewall-1 product consists of 3 interrelated components. These are Management Module, Enforcement Module and GUI Clients as depicted below:



- **Management Module (SmartCenter Server)**

The Management module stores the Security Policy and is responsible for holding the Logs, the User database and Network objects used by the security policy. The management module moves these functions away from the enforcement modules, thereby freeing up resources on the enforcement modules and improving performance. Also the management module can be utilised to maintain the logs and policies for numerous enforcement modules, hence simplifying the management of the firewall infrastructure.

- **Enforcement module (EM)**

The Enforcement module is the sharp end of the infrastructure. It is responsible for inspecting the traffic at the network gateway and enforcing the security policy on that traffic. As such, this is the component that actually performs the firewalling functions. There can be one or more enforcement modules in a Firewall-1 configuration managed by one central management server. For the purposes of this document, enforcement modules will be referred to in the singular, for ease of understanding.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- **GUI Client**

The GUI Client is used to configure the management module and provides a simplified graphical interface for carrying out configuration tasks. This is made up of a number of discrete interfaces, as listed below:

1. SmartDashboard – Used to configure the Object database and Rulebase
2. SmartView Tracker – For viewing the firewall logs.
3. SmartView Monitor – Holds Infrastructure Performance indicators and usage statistics.
4. SmartView Status – Displays information of system status (up/down) and health checks for all infrastructure devices.
5. SmartView Reporter – Provides graphical reporting on firewall usage.

All three components above may reside on the same machine, or may be distributed in different physical locations. The benefits of a distributed architecture come to the fore when deployed in a larger enterprise with multiple enforcement modules and multiple firewall administrators. Where the components are distributed they use SIC (Secure Internal Communication) to encrypt and validate traffic that passes between them. SIC uses an Internal PKI (Public Key Infrastructure) to authenticate each module, apply access control and encrypt the traffic between modules.

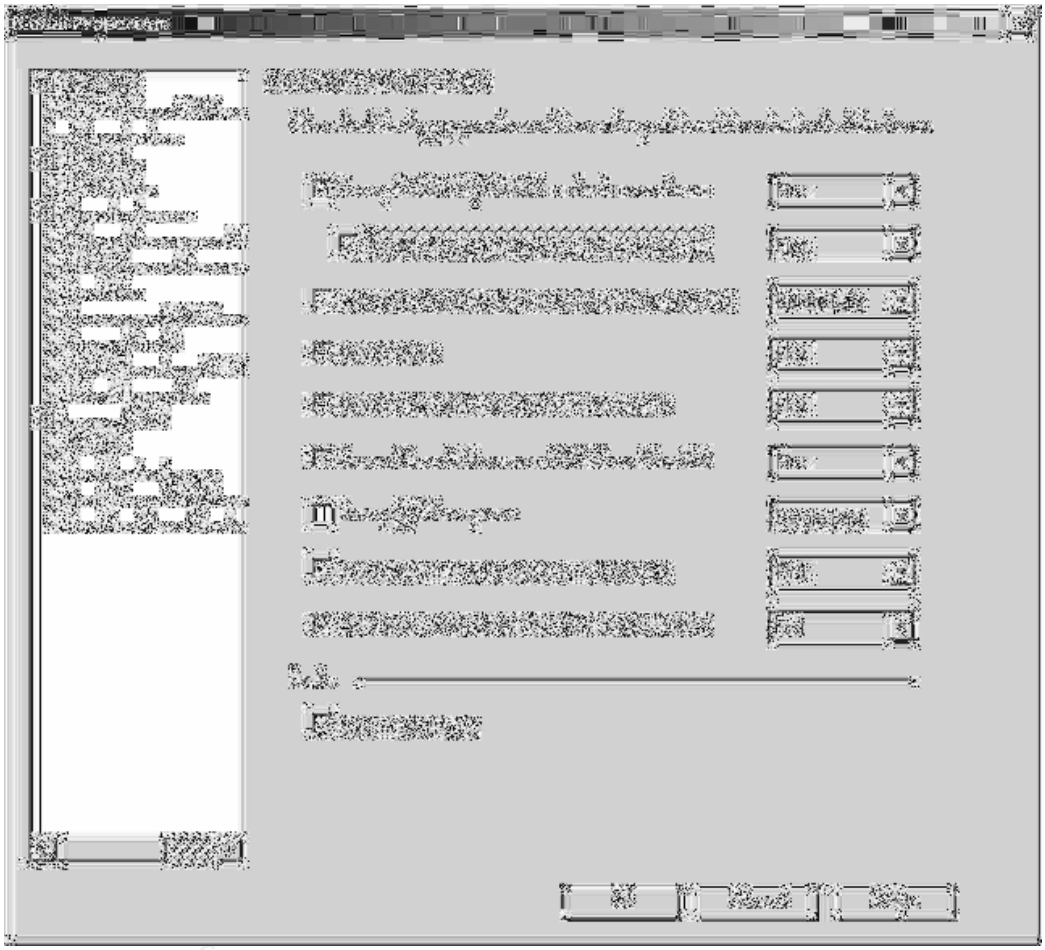
The Firewall-1 product also provides a VPN Solution (called VPN-1) for remote user connectivity and also a point-to-point VPN Solution for connecting disparate offices. These VPN configurations are also configured and maintained using the same 3-tiered architecture described above.

In 1997 OPSEC *(CHECKPOINT, 8)* (Open Platform for Security) was created by Checkpoint as a framework of inter-operability for security application and appliance vendors. This allows third party products such as Anti-Virus, Content filtering and Intrusion detection to integrate with Checkpoint's products to provide combined and integrated security solutions.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction to Implied Rules.

On configuring the firewall-1 product, a large number of implied firewall rules can be generated by the product itself. These rules are automatically created in the rulebase and cannot be edited, or individually deleted. By default, these rules are hidden from view. They are based on the settings selected in the Global Settings of the SmartDashboard Software (Policy > Global Properties).



The implied rules consist of firewall rules, which specifically allow certain TCP or UDP traffic to pass through the enforcement module enabling the various components of the Firewall-1/VPN-1 solution to interact.

The rules control communication between the Management module, enforcement module(s) and GUI Client(s) as well as controlling other functions such as VPN authentication traffic and OPSEC compatible server integration traffic.

To view the implied rules log onto the SmartDashboard and select View > Implied Rules. Depending on the selections made in the Global Properties a potentially large number of extra rules will appear in the rulebase alongside administrator configured rules.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Best Practice

Best practice in firewall implementation is described in the Policy Considerations section of the CERT Practice document 'Configure Firewall Packet Filtering'. This states:

"That all network traffic that is not explicitly permitted should, by default, be denied." (CERT, 3)

This is clarified by Checkpoint themselves, as is stated in their document 'Check Point VPN-1 & FireWall-1 NG Performance Tuning Guide'

"Disable any FireWall-1 implied rules that you do not need." (CHECKPOINT, 4)

This best practice leaves the administrator of a firewall in a dilemma. The Firewall-1 products' implied rules explicitly permit certain traffic, which may or may not be desired in a live, operational environment and may even reduce the effectiveness of the firewall leaving unused ports open and the trusted network more vulnerable to attack.

It would seem appropriate and within the guidelines of best practice, then, to disable ALL settings which generate these implied rules and manually configure the rulebase to specifically allow only traffic that is essential for the Firewall infrastructure to operate effectively in the environment.

Implied Rules in detail.

Below are detailed the rules that are created when selections are made in the Global Properties of Firewall-1 (Policy>Global Properties). The selections that can be made are listed below:

- Accept VPN-1 & Firewall-1 control connections
    - Accept Remote Access control connections
- Accept Outgoing packets originating from Gateway
- Accept RIP
- Accept Domain Name over UDP (Queries)
- Accept Domain Name Over TCP (Zone Transfer)
- Accept ICMP Requests
- Accept CPRID Connections (Smart Update)
- Accept Dynamic Address Modules' DHCP Traffic.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. **Accept VPN-1 & Firewall-1 control connections**
    a. **Accept Remote Access control connections**

The implied rules created by these selections control communications between the daemons, or services, that Firewall-1 uses on different machines (SmartCenter server, management client and enforcement module). They also control connections with external servers, such as RADIUS and TACACS servers for authentication, and also external machines for extranet configuration. Other rules created relate to VPN communications with Checkpoint SecuRemote clients and SecureClient software.

Depending on the configuration of ones firewall infrastructure, some of the implied rules created are required, whilst others may not be. For example, where the enforcement module is being used solely as a firewall and is not for VPN functionality, some of these rules can be disabled whilst still keeping all the functionality of the firewall. If the management and enforcement functionality of the Firewall Infrastructure (i.e. the management server and the enforcement module) reside on the same machine, again some of these rules may be disabled.



The above rules are created to allow communications between the 3 components of the Firewall-1 infrastructure. The rules allow traffic over TCP ports 256, 18191, 257, 18190 and 18202. These rules are required for communication to occur where the Management module, enforcement module(s) and GUI Client(s) do not reside on the same machine.

- The FW1 service (TCP port 256) is responsible for communication of the firewall rulebase and for communicating topology information. *(AERASEC,* 5)
- The CPD service (TCP port 18191) is used by the Management module to 'fetch' the firewall rulebase from the enforcement module when the management module is started. *(AERASEC,* 5)
- The FW_log service (TCP port 257) is used to deliver Firewall logs from the enforcement module to the Management module. *(AERASEC,* 5)
- The CPMI service (TCP Port 18190) is used to communication between the GUI Clients and the management module. *(AERASEC,* 5)
- The CP_rtm service (TCP port 18202) is used for the management console to communicate information to the Real time monitor (Checkpoint SMARTView Monitor). *(AERASEC,* 5)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

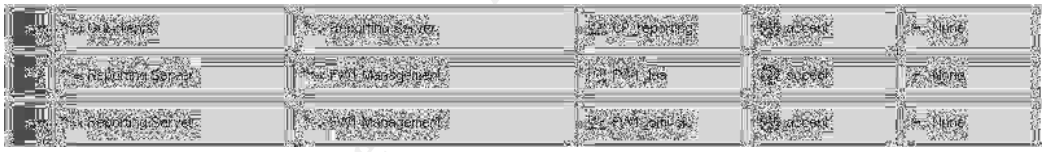
Where the management module, enforcement module and GUI Client are on the same machine, all the above rules can be disabled. If the GUI Client resides only on the same machine as the management server (for example if administrators connect to the management server using RDP (Remote Desktop Protocol) then the Rule denoting CPMI can be disabled as no network communication occurs from GUI Clients to the management module.



These rules are used for VPN Implementation from Firewall-1.

- FW1_topo service (TCP port 264) is used by SecureClient and SecuRemote to download topology information from the enforcement module or the management module. *(AERASEC,* 5)
- FW1_key service (TCP port 265) is used by SecureClient and SecuRemote to download Public Keys from the Management module. *(AERASEC,* 5)

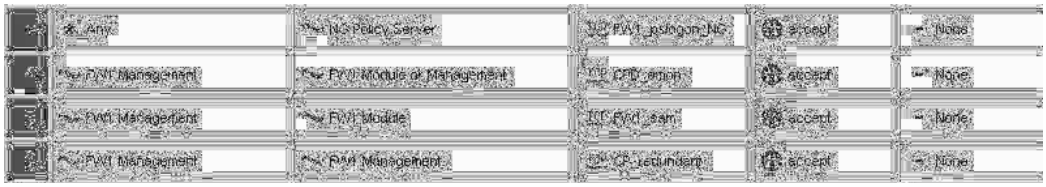
If VPN is not implemented in the Infrastructure, these rules can be disabled.



- CP_reporting service (TCP port 18205) is used by GUI Clients to connect to the SmartView reporter. *(AERASEC,* 5)
- FW1_lea service (TCP port 18184) is used for communication with logging and event APIs, third party OPSEC applications which receive and process logging information. *(ALEX BUTCHER, 9)*
- FW1_omi_sic (TCP port 18186) is used by 3rd party OPSEC servers to connect to the management module with secure (SIC) communication. *(AERASEC,* 5)

The first rule above may be disabled if the GUI Clients reside on the same server as the Management module.
The latter two rules may be disabled if no 3rd party OPSEC compliant services are used.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



- FW1_pslogon_NG service (TCP port 18231) is used in VPN implementation by SecureClient to download Desktop security policy to the remote desktop machine. *(AERASEC,* 5)
- CPD_amon service (TCP port 18192) is used to deliver system status information from the Management module to the enforcement module. *(AERASEC,* 5)
- FW1_sam service (TCP port 18183) is for OPSEC compliant 3rd party applications to block traffic from the Management module to the enforcement module. This is known as the Suspicious activity monitor and will block suspicious traffic that would normally be allowed by the firewall rulebase. *(AERASEC,* 5)
- CP_redundant service (TCP port 18221) is used to synchronise primary and secondary Management modules. *(AERASEC,* 5)

The first rule above may be disabled if there is no VPN implementation or if Secure Client is not used. The Second rule above may be disabled if the management module and the enforcement module reside on the same machine. The third rule may be disabled if there is no usage of 3rd party OPSEC services and the fourth rule may be disabled if there is only one primary Management module within the infrastructure (there is no requirement for synchronicity with a secondary Management module).



These rules are related to VPN implementation and allow any computer to access the local machine (the enforcement module) using UDP port 500. This allows implementation of IKE for VPN Clients.
IKE is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE. *(CISCO, 10)*
If VPN functionality is not implemented, these rules can be disabled.

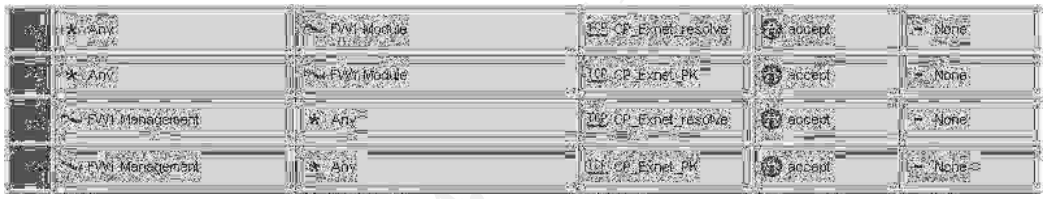
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



The above rules are created to enable the pushing and pulling of Internal CA certificates between management module and the Enforcement modules for the purposes of Secure Internal Communication (SIC).

- FW1_ica_pull service (TCP port 18210) is used by SIC to pull Certificates from the management module. *(AERASEC,* 5).
- FW1_ica_push service (TCP Port 18211) is used by SIC to push certificates to the enforcement module from the management module. *(AERASEC,* 5)

These rules are only required when the Enforcement module and the management server reside on separate machines. SIC is not required when the modules do not communicate over the network. They can therefore be disabled in these instances.



The above rules are used for controlling connections when an extranet is configured.

- CP_Exnet_PK (TCP port 18262) service allows the exchange of public keys with extranet partners. *(AERASEC,* 5)
- CP_Exnet_resolve (TCP port 18263) service allows the importing of exported firewall objects from the extranet partner and vice versa. *(AERASEC,* 5)

These rules can be disabled when an extranet is not in use.

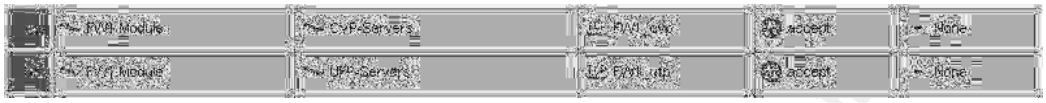


This is another rule configure for VPN communication.

- RDP service (UDP port 259) allows VPN Clients to authenticate to the enforcement module using FWZ *(CHECKPOINT, 6)* Key Management.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

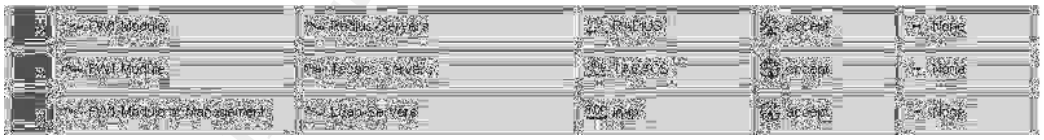
This appears to be an obsolete rule as in Firewall-1 NG FP2 and beyond VPN clients use IKE, not FWZ to authenticate. *(CHECKPOINT, 7)* In any case if VPN's are not used, this rule can be disabled.



These 2 rules relate to third party Servers that add 'outsourced' functionality to the Firewall-1 Infrastructure through OPSEC. *(CHECKPOINT,* 8)
CVP (Content Vectoring Protocol) Servers provide Anti-Virus functionality to the firewall infrastructure.
UFP (URL Filtering Protocol) Servers provide content filtering of URL's to the Firewall infrastructure.

- FW1_cvp service (TCP port 18181) provides communication between the enforcement module and CVP servers providing 3rd party anti virus filtering. *(AERASEC,* 5)
- FW1_ufp service (TCP port 18182) allows the enforcement module to communicate with 3rd party UFP Servers which provide Content filtering services. *(AERASEC,* 5)

These two rules may be disabled if there are no 3rd party OPSEC compliant servers within the firewall infrastructure.



These three rules relate to User Authentication, particularly for Remote VPN users. They allow the enforcement module to authenticate users against third party RADIUS, TACACS or ldap servers.

- RADIUS service (UDP port 1645) allows communication with RADIUS (Remote authentication dial in user service) Servers. *(AERASEC,* 5)
- TACACS Service (UDP port 49) allows communication with TACACS (Terminal Access Controller Access control System) Servers. *(AERASEC,* 5)
- ldap Service (TCP Port 389) is used by the management console or the enforcement console for communication with ldap databases to assist authentication of VPN Users, but also for enforcing firewall rules to users contained in a third party ldap database, such as Windows 2000 Active Directory. *(AERASEC,* 5)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

If RADIUS or TACACS servers are not used for authentication, these rules can be disabled. Communication with an ldap server may be desirable for assisting in applying firewall rules on a per-user basis, however if this is not used, this rule can be disabled also.



- tunnel_test service (UDP port 18234) is used by SecuRemote and SecureClient for testing applications through a VPN connection. *(AERASEC,* 5)

1. Accept Outgoing packets originating from Gateway



This rule allows any traffic (any protocol, any port) deriving from the Gateway machine (the Firewall-1 enforcement module) to any destination to be accepted by the firewall. This could cause problems should an enforcement module become compromised in which case there is no restriction on what an attacker could do from the compromised machine. The recommended setting from Checkpoint is that this rule is disabled in the Global Properties of the firewall.

3. Accept RIP



- RIP Service (UDP port 520) is the Routing Information Protocol. RIP is used to communicate information about reachable systems and the routes used to those systems. The recommended setting from Checkpoint is that this rule is disabled in the Global Properties of the firewall.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4. Accept Domain Name over UDP (Queries)



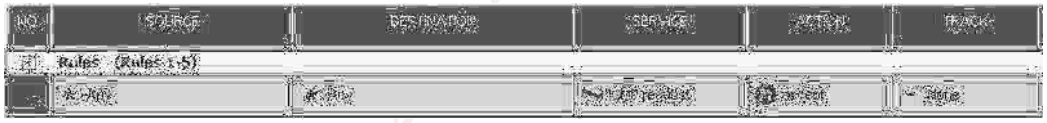
domain_udp service (UDP port 53) serves DNS requests to allow hostname to IP address resolution. Checkpoint recommends this rule be disabled.

5. Accept Domain Name Over TCP (Zone Transfer)



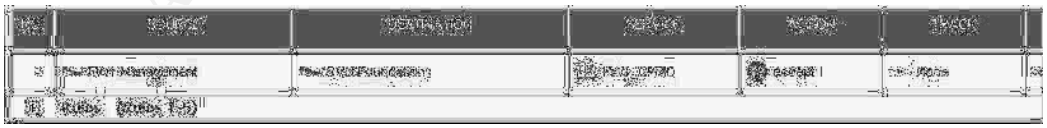
domain_tcp service (TCP port 53) serves DNS requests over TCP. This protocol is used to download name resolving tables when zone transfers occur between servers. Checkpoint recommends this rule be disabled.

6. Accept ICMP Requests



This rule allows ICMP (Internet Control Message Protocol) traffic, such as PING to pass across the gateway. Checkpoint recommends disabling this rule.

7. Accept CPRID Connections (SmartUpdate)



This rule allows SmartUpdate connections. SmartUpdate is functionality within the firewall-1 product that allows the latest hotfixes, service packs and updates to be applied remotely and automatically to Firewall-1 components such as the Management modules and the enforcement modules.

- FW1_CPRID service (TCP port 18208) Is the Checkpoint Remote Installation Protocol. *(AERASEC,* 5)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This rule should be enabled if SmartUpdate functionality is used in the infrastructure. If manual updates are applied, then this rule can be disabled.

8. Accept Dynamic Address Modules' DHCP Traffic.



This rule allows DHCP traffic from enforcement modules to be passed in order for them to obtain a DHCP supplied IP Address where the module is configured to receive a dynamically assigned IP Address.
If all modules in the infrastructure have statically assigned IP addresses, then this rule can be disabled.

Disabling and Recreating Implied Rules.

When a decision has been made about which implied rules need to be retained for correct functionality, these rules need to be recreated in the rulebase and the Global Properties selections disabled.

To disable the implied rules, log on to the SmartDashboard and select the Policy menu > Global Properties. Under Firewall-1 untick all the boxes on the Firewall-1 Implied Rules page. All implied rules will now be disabled. You can check this is the case by selecting the View > Implied Rules menu. The rulebase should only show administrator configured rules.

To recreate the rules that are required, objects must be created in the objects database, which correspond to the objects in the firewall-1 infrastructure. These may include, management modules, enforcement modules, GUI Clients, RADIUS Servers, TACACS servers, Reporting Servers, Policy Servers. DHCP Servers, DNS Servers, CVP Servers, UFP Servers, ldap servers.

© SANS Institute 2004, Author retains full rights.

These objects can then be added to a rule in the usual way. For example to enable the following rule:

-	FW1 Module or Management	FW1 Module or Management	TCP FW1	accept	- None

Each enforcement module and management module has an associated object created in the object database. A rule is then created with the new objects as source and destination accepting the FW1 Service (TCP Port 256).

For scalability, it may be advisable to create groups containing the objects. This will allow for easy integration of any further enforcement modules or management modules. If a further module is subsequently brought online, a corresponding database object can be added to the appropriate group and the rules will be applied correctly to the new module. This can be seen in the image below where the source contains a group of management modules and the destination is a group containing firewall modules (enforcement modules).



Image courtesy of http://www.phoneboy.com/bin/view.pl/FAQs/GlobalPropertiesNG
(PHONEBOY, 11)

Care must also be taken to ensure the rules are in the correct position in the rulebase. The majority of implied rules are positioned above rule 1 in the rulebase although this is not always the case and so, prior to disabling the implied rules, the position of the rules being replaced relative to each other must be noted.

Following replacement of the implied rules it would also be wise to log dropped traffic on the firewall by the default rule. The logs can then be inspected to establish if there is any traffic being dropped on the implied rules' ports. This would help ascertain if indeed some of the rules that have not been recreated are required and in use and would be especially useful in troubleshooting any firewall issues that may arise as a result of replacing the implied rules. If so, it may be worth considering creating a rule to allow that traffic to ensure the infrastructure is communicating correctly.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix 1 – Ports Used by implied rules

Service Name	Description	Protocol	Port
FW1	Checkpoint VPN1 &Firewall-1 Service	TCP	256
CPD	Checkpoint Daemon Protocol	TCP	18191
FW1_log	Checkpoint VPN-1 &Firewall-1 Logs	TCP	257
CPMI	Checkpoint Management Interface	TCP	18190
CP_rtm	Checkpoint Real Time Monitoring	TCP	18202
FW1_topo	Checkpoint VPN-1 SecuRemote Topology Requests	TCP	264
FW1_key	Checkpoint VPN-1 Public Key Transfer Protocol	TCP	265
CP_reporting	Checkpoint Reporting Client Protocol	TCP	18205
FW1-lea	Checkpoint OPSEC Log Export API	TCP	18184
FW1_omi-sic	Checkpoint OPSEC Objects Management Interface with Secure internal communication	TCP	18186
FW1_pslogon_NG	Checkpoint NG Policy Server Logon Protocol	TCP	18231
CPD_amon	Checkpoint Internal Application Monitoring	TCP	18192
FW1_sam	Checkpoint OPSEC Suspicious Activity Monitor	TCP	18183
CP_redundant	Checkpoint Redundant management protocol	TCP	18221
IKE	IPSEC Internet Key exchange Protocol (formerly ISAKMP/Oakley	UDP	500
FW1_ica_pull	Checkpoint Internal CA Pull Certificate service	TCP	18210
FW1_ica_push	Checkpoint Internal CA Push Certificate Service	TCP	18211
CP_Exnet_Resolve	Checkpoint Extranet remote objects resolution	TCP	18263
CP_Exnet_PK	Checkpoint Extranet public key resolution	TCP	18262
RDP	Checkpoint VPN-1 FWZ Key Negotiations - Reliable Datagram Protocol	UDP	259
FW1_cvp	Checkpoint OPSEC Content Vectoring Protocol	TCP	18181
FW1_ufp	Checkpoitn OPSEC URL Filtering Protocol	TCP	18182
RADIUS	Remote Authentication Dial-In User Service	UDP	1645
TACACS	Terminal Access Controller Access Control System over UDP	UDP	49

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ldap	Lightweight Directory Access Protocol	TCP	389
tunnel_test	Checkpoint tunnel testing application	UDP	18234

© SANS Institute 2004, Author retains full rights.

Glossary of Terms – All definitions taken from www.webopedia.com [12]
N.B. All terms contain active links to their respective definition at www.webopedia.com.[12]

PKI - Short for *public key infrastructure,* a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread.
A PKI is also called a *trust hierarchy.* [13]

RADIUS - Short for ***R****emote* ***A****uthentication* ***D****ial-****I****n* ***U****ser* ***S****ervice,* an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Though not an official standard, the RADIUS specification is maintained by a working group of the IETF. [14]

RIP – **(n.)** Abbreviated as *RIP*, an interior gateway protocol defined by RFC 1058 that specifies how routers exchange routing table information. With RIP, routers periodically exchange entire tables. Because this is inefficient, RIP is gradually being replaced by a newer protocol called Open Shortest Path First (OSPF). [15]

TACACS - Short for ***T****erminal* ***A****ccess* ***C****ontroller* ***A****ccess* ***C****ontrol* ***S****ystem*, an authentication protocol that was commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.
TACACS is now somewhat dated and is not used as frequently as it once was. A later version of TACACS was called XTACACS (E**x**tended). These two versions have generally been replaced by TACACS+ and RADIUS in newer or updated networks. TACACS+ is a completely new protocol and is therefore not compatible with TACACS or XTACACS.
TACACS is detailed in RFC 1492. [16]

VPN - Short for ***v****irtual* ***p****rivate* ***n****etwork,* a *network* that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.[17]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

1. Checkpoint Web Site
   http://www.checkpoint.com/products/supported_platforms/platforms_appint.html
   (June 29 2004)

2. Webopedia Website
   http://www.webopedia.com/TERM/S/Stateful_Inspection.html
   (June 30 2004)

3. Cert Website, "Configure Firewall Packet Filtering", Cert Security Improvement modules, July 1 1999.
   http://www.cert.org/security-improvement/practices/p058.html
   (June 29 2004)

4. Checkpoint Website
   http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html
   (June 30 2004)

5. Aerasec, "TCP and UDP ports used by Next Generation", Checkpoint VPN-1/Firewall-1, April 11 2004
   http://www.fw-1.de/aerasec/ng/ports-ng.html
   (June 30 2004)

6. Checkpoint website, "FWZ", Virtual Private Networks and Enterprise Security
   http://www.checkpoint.com/vpnguide/f.html
   (June 30 2004)

7. Checkpoint Website , "VPN-1 Migration from FWZ HotFix for NG FP2". April 2002.
   http://www.checkpoint.com/techsupport/downloads/html/ng_fp2/fp2_fwz_hf_release_notes.html
   (June 30 2004)

8. Checkpoint Website, "Build your Security Infrastructure With Best-of-Breed Products from OPSEC". 2004
   http://www.checkpoint.com/products/downloads/opsec_whitepaper.pdf
   (July 1 2004)

9. The Internet Ports Database, Alex Butcher, July 2 2004
   http://www.portsdb.org/bin/portsdb.cgi?name=Alex%20Butcher
   (July 2 2004)

10. Cisco Website, "Internet Key Exchange Security Protocol", Documentation, Feb 3 2004.
    http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/isakmp.htm - xtocid0
    (July 2 2004)

© SANS Institute 2004, Author retains full rights.

11. Phoneboy Dot Com Website, “How can I disable everything in the rulebase properties in VPN-1/FireWall-1 NG?”, Jan 14 2004 http://www.phoneboy.com/bin/view.pl/FAQs/GlobalPropertiesNG (July 2 2004)

12. Webopedia Website www.webopedia.com (July 2 2004)

13. Webopedia Website, “PKI” http://www.webopedia.com/TERM/P/PKI.html (June 30 2004)

14. Webopedia Website, “RADIUS”. http://www.webopedia.com/TERM/R/RADIUS.html (June 30 2004)

15. Webopedia Website, “Routing Information Protocol” http://www.webopedia.com/TERM/R/Routing_Information_Protocol.html (June 30 2004)

16. Webopedia Website, “TACACS” http://www.webopedia.com/TERM/T/TACACS.html (July 1 2004)

17. Webopedia website, “VPN” http://www.webopedia.com/TERM/V/VPN.html (July 2 2004)

© SANS Institute 2004, Author retains full rights.