Technical Incursion Countermeasures

The Firewall Hardening Guide v0.1 - Index

The Firewall Hardening Guide v0.1 - Administrative

0.0 Information related to this FAQ

The official home for this FAQ is Technical Incursion Countermeasures, http://www.ticm.com/info/insider/members/FW1SecGuide/index.html

0.1 Legal

1. This text is not an endorsement for any product.
2. It is not cookbook to be used by crackers to gain access to firewall systems.
3. I am affiliated with TICM and from time to time various clients. I am not affiliated with any of the vendors mentioned in the FAQ (though I'm always open to offers :}).
4. All trademarks are the property of their owners.
5. All included material are copyrighted by their respective owners/copyright holders.
6. This compilation is copyrighted material. Copyright © 1999 Bret Watson. You are hereby granted a
7. permission to use the material for non-commercial purposes as long as you keep this copyright message, not pretend
8. that you wrote the material and give me and/or the other contributors proper credits.

0.2 Current version and updating information

The current version number of the FAQ is 0.1 The FAQ was last updated 29th of October 1999. Please submit contributions and requests for updates to the current maintainers (faq@ticm.com) of the FAQ.

Technical Incursion Countermeasures

The Firewall Hardening Guide v0.1 - Introduction

Introduction

FW-1 Overview

Check Point FireWall-1 is a software firewall product that uses Stateful Inspection Technology, which was invented and patented by Check Point. FireWall-1 inspects all packets passing between networks connected to the product, blocking all unwanted communication attempts. It supports the comple-te TCP/IP family of protocols.
The packet inspection is based on information contained in protocol headers and the state information derived from one or more associated packets. FireWall-1 can therefore be configured not only to in-spect individual IP packets based on the IP header information, such as source and destination IP ad-dresses, but also to examine state information in multiple IP packets.
FireWall-1 provides IP address translation that permits selected internal network addresses to be hidden from the external network so that only the internal network hosts are able to initiate communica-tions. FireWall-1 also provides source and destination address translation, to overcome the limitation of the number of IP addresses on the Internet.
FireWall-1 may be configured to operate connected to one external (public or unprotected) network and up to 31 physical internal (protected) networks. FireWall-1 is managed locally via a workstation or con-sole directly connected to the firewall.

The Firewall Hardening Guide v0.1 - Generic Firewall Requirements

Mandatory Requirements

These requirements are mandatory to ensure a secure firewall system.

Network Documentation

All network related documentation must be updated and currency of content maintained. Network related documentation should be appropriately identified with date, version number, and commentary as to what changes have been made to the content. All such changes should be managed via a formal change control mechanism. In order to ensure that the firewall is securing the required section of the network a detailed diagram of the network may be required. This can be used to ensure that the firewall is protecting what it should be protecting and will help in identifying any weaknesses that may exist within the firewall setup.

Change Control

Management should document a formal change control policy for amending the firewall's configuration. This policy should describe the principles and objectives on which change control process should op-erate. Having defined when changes should be performed, the objectives should describe change re-quirements (that is-key standards). Change Control is required to ensure that administrators of the firewall are in fact performing the task required of them. This is done to
1. ensure changes made reflect the change in policy.
2. ensure the administrators do not perform changes without notification.
Non conformance may result in loss of control over changes to network devices resulting in unauthorised access into a device and the potential for an unauthorised person to alter security configuration parameters.
Personnel installing changes must be authorised to do so and held accountable for the change. If the organisation does not identify the authorised individuals who update the firewall, the risk increases of unauthorised changes to configurations

Firewall Documentation

Firewall documentation should exist, and as a minimum detail the firewall policy and the rational for the inclusion of each individual rule. Documentations should also justify the exclusion of specific rules, where the absence impacts on the security of the firewall and/or the corporate network. In order

to de-sign a rule base it is important to have supporting documentation outlining the policies required by the organisation. These should be kept up to date to reflect the actually policies in place on the firewall(s).

Physical Security

Ensure that the Firewall and the network cabling related to it are physically secured. Physical access to the firewall or the related network cabling provides opportunities for an intruder to bypass the firewall itself.

Patches

Ensure that patches to the base operating system and to the firewall are current. For a firewall to be successful it must operate on a secure operating system. If the firewall is running on an inferior system then it is open to attacks not possible according to the firewall. It should be ensured that the system the firewall is run on is secure and that all patches have been applied.

Backup Procedures

Ensure that backup procedures exist for the firewall configuration and the log files. The firewall should be backed up to ensure quick recovery from data loss. The log files should be archived separately to ensure a permanent record of transactions. The archived logfiles should be removed from the firewall as they will slowly consume all available space on the system, potentially causing failures. There should be sufficient space for the log files to reduce the risk that the partition will be deliberately filled by an attacker.

Alert Procedure

If Alerts are enabled then there should exist a documented procedure for handling the alert

The Firewall Hardening Guide v0.1 - Generic Firewall Requirements

Recommended Requirements

These requirements are strongly recommended, however it is recognised that these are not possible in all instances. Failure to comply to these requirements may degrade the security of the firewall.

Testing Procedures

It is recommended that procedures exist for testing the firewall before it is the changes are installed on the firewall. If the firewall policy is altered then there need to be a process where by the new policy is tested before it is 'burnt' into the actual firewall. This is done to ensure that the changes to the firewall do not have a negative effect on its operation.

User names / passwords for managing the firewall.

Windows NT is not considered secure when unauthorised people get physical access to the com-puter. This includes the ability to obtain usernames/passwords (using tools like NTFSdos and L0phtcrack), and if such tools as MS SMS, PC anywhere etc. are being used for managing the com-puter, others may watch the local console monitor to obtain and possibly also interrupt the remote man-agement session. Few people (1-5) should be allowed access to the firewall. This includes physical access, local logon (Windows NT) and remote firewall logon. Windows NT remote access should not be allowed.
Hard-to-guess usernames and password should be used. Each user with read or read/write access to the firewall configuration should be identified by unique usernames.

Management stations that can access and configure the firewall

During installation you must set DNS host names and/or IP addresses of those man-agement stations allowed to access the firewall. We recommend using IP addresses instead of DNS host names, as this increases the risk of spoofed DNS attacks to the firewall management ports.

The Firewall Hardening Guide v0.1 - Checkpoint Firewall-1 Specific Requirements

Log and alert

Excessive Log Grace Period (sec)

This specifies the minimum amount of time between consecutive logs of similar packets. Higher number means less logging, and a higher risk of 'losing' important information.
If log analysis is being performed, lowering this parameter value will help improving the accuracy of the log analysis when searching for portscanning attempts and doing performance/usage analysis. This value should be experimented with; we recommend a setting at 30 seconds or lower if pos-sible.

Popup Alert Command

This specifies the command to be executed when an alert is issued. Default value is ok, unless another specific action is wanted.

Mail Alert Command

This specifies the command(s) to be executed when Mail is specified as the required alert action. Remem-ber: it may take some time before the recipient receives a mail message, and the message must also be read.
Default setting is to send mail to the local root account, which normally won't exist on the system (…). IF there is a system for transferring SMTP mail available, 'root' should be changed to 'name-of-person-responsible@Company.com'. Note: On NT machines there is no mechanism by default for sending mail. One will have to be installed – this should be done before the firewall is installed to reduce the possibility of vulnerable services being exposed.

SNMP Trap Alert Command

Specifies the command to be executed when SNMP is specified as the required action. Remember that SNMP and SNMP traps are UDP based services, and does not require a confirmation from the recip-ient of such an alert message. The default value is also set to send such SNMP Traps to 'localhost', which is the firewall system itself. This setting should be changed. Instead of localhost, an IP address of an SNMP control unit (such as CA Unicenter etc….) should be inserted.
Do not use DNS names, because doing so may allow an attacker to trick the firewall to send the SNMP Trap message to the wrong recipient station, due to failures or spoofed DNS information.

User Defined Alert Command

Specifies the command to be executed when “User-Defined” is defined as the required alert action. This setting may be used for invoking third-party applications, such as pager messages or SMS messages to a cellular phone.

Anti Spoof Alert Command

Specifies the command(s) to be executed when alert is specified for anti-spoofing detection in the Net-work Interfaces section of the HOST PROPERTIES window.
Spoofing will normally be an attempt to trick the firewall to accept a packet from one interface, and des-tined for another interface, where the IP packet seems legitimate because of a faked sender IP ad-dress.
Attempts on using spoofed IP addresses should be detected by configuring anti-spoofing for every interface in the firewall configuration (Firewall-1 object definition – Interfaces), and should be alerted if detected.
This value may contain an SNMP trap alert, or e-mail alert, or another third-party application/solution.

User Authentication Alert Command

Specifies the command(s) to be executed when alert is specified for Authentication failure track in the Control Properties/Authentication window. If a user database is being managed and used in conjunc-tion with Firewall-1’s user authentication abilities, this option should be properly configured to give some kind of alarm, such as SNMP Traps, e-mail notification or third-party applications/solutions.

IP Options Drop Track

IP packets containing data in the options field will always be dropped (ie. ignored) by Firewall-1, but such packets should be logged, or also generate an alarm.
This value should be set to ‘log’, or in a high-security environment ‘alert’.

Log established TCP Packets

Enables logging of TCP packets previously established, or packets whose connections have timed out. This option should be enabled.

Log ISAKMP negotiations

This option should be enabled.
This will enable logging of ISAKMP negotiations. By analyzing these log events, it will be possible to do usage monitoring.

Log encryption kernel events

This option will enable logging of encryption events. This option may be disabled, as we see no immediate danger of not logging legal encryption events. This option may be enabled for debugging purposes, when troubleshooting encryption installations.

Enable Active Connections (This option has been removed from V4.x)

Enables live connections to be viewed from the Log Viewer for Firewall-1. Represents no security risk. This option should be enabled.

The Firewall Hardening Guide v0.1 - Checkpoint Firewall-1 Specific Requirements

Services

Enable FTP PORT Data Connections

This setting enables the use of FTP through Firewall-1.
We recommend that this setting should be enabled, provided internal users are allowed to do file downloading using FTP clients.

Enable FTP PASV Connections

This setting enables web browsers to do FTP downloads. Most (if not all) web browsers today, including Internet Explorer and Netscape uses FTP PASV connections for their file transfers (FTP://…..). FTP PASV connections represent a higher security risk under certain conditions, and should be applied carefully.
We recommend that this setting should be enabled, provided internal users are allowed to do file downloading using their web browsers.

Enable RSH/REXEC Reverse stderr Connections

Allows RSH and REXEC to open reverse connections for the stderr file. Enabling these services may represent certain security risks, and should be applied carefully.
This setting should be disabled, unless there exists a documented need for these services.

Enable RPC control

Enabling Remote Procedure Call may represent certain security risks, and should be applied carefully. RPC may be used to obtain information on what services are running (=available) on a given host.
This setting should be disabled, unless there exists a documented need for these services.

The Firewall Hardening Guide v0.1 - Checkpoint Firewall-1 Specific Requirements

Miscellaneous

In this section we have only provided information on those settings that applies to a minimum security guideline, and needs to be changed from the default values. Most of the settings in these areas does not represent any security risks, and may be left at their default values unless specifically needed in accordance with extra modules for Firewall-1.

Lookup Priorities

This is our recommended setup:
1. HOSTS (if file exists, and is being used)
2. SYS (Current System Setting)
3. BIND (Internet DNS, will utilize those settings found in TCP/IP properties of Windows NT)

Log Viewer Resolver Properties

Only applies if DNS resolving is being used within the Log Viewer itself. We recommend to turn off DNS resolving within the Log Viewer, and instead use a third-party application for Firewall-1 log analysis.
Default value may be lowered to 6-12 seconds, depending on Internet connection speed, and distance (router hops) to closest DNS server.

Access List settings

Only applies to Firewall-1 installations where a router control module is installed, and should be configured in accordance with the general access lists implemented in both internal and external rout-ers.
(Recommendations on router configuration is not a part of this document)

Security server settings

If the GM site chooses to utilize security servers for Telnet, FTP or Rlogin, remember that Firewall-1 will announce its presence upon login. This banner information reveals the firewall type to (un)authorised users, any may pose a security risk.
If applied, welcome files should contain warnings about unauthorised use and that all transactions are

being logged as a minimum.
Authentication settings: Authentication failure track should be set to ‘Log’ as a minimum, or Alert in high-security environments.
Miscellaneous settings:
(no comments)

SYNDefender settings

A SYN attack work by sending large amounts of SYN requests, where the sender IP address is spoofed (ie. fake, non-existing address). These packets may in certain environments slow down or crash the operating system.These options were inroduced in version3 of Firewall-1. Most (if not all) systems today are well-protected against SYN attacks.
Our recommended settings are:
Method: SYN Gateway
Timeout: 10 seconds
Maximum sessions: 5000
Display warning messages: YES (enabled)
If such warning messages occur, it may be an active SYN flood attack. By inspecting the IP packets (using a packet sniffer on the ‘attacked’ segment) for source port numbers and source IP address, ac-cess lists in the external router may be applied to:
Stop IP packets with a specific source port number (unless the attacker is using random source ports)
Stop IP packets that have a non-existent IP address as its source address

The Firewall Hardening Guide v0.1 - Checkpoint Firewall-1 Specific Requirements

Suggested Rules

Tracking

All firewall rule tracking should be set to long The rule tracking facility provides a logging mechanism for tracking the triggering of rules. There are three options available: None, short and long. Long pro-vides detailed logging of triggered rules, whilst short gives a basic record.

DNS queries from internal hosts (clients)

As described in xxx, DNS queries are disabled through the control properties. This is done mainly to prevent internal hosts to communicate with the outside world by running standard applica-tions (Telnet etc..) through the Firewall-1 using the DNS port, TCP port 53. If this isn't disabled, internal users may get access to systems on the Internet, without the firewall being able to log or detect this activity.
Internal clients (workstations and servers) should only depend upon an internal DNS server. Inter-nal clients will not be able to access anything on the outside using TCP or UDP port 53, the normal DNS ports.
An internal DNS server acting as a 'caching only' should be installed, and this server should be the only one allowed to use the DNS ports through the Firewall-1. All internal DNS requests must be sent to this computer.
The following rule should be installed:
Source: Internal DNS server
Destination: Internet
Service DNS (UDP port 53)
Action: Allow
Track: (log during installation, after confirmed operation may be set to no log)
Time: Any

DNS queries from internal (DMZ) DNS servers to the outside (Internet)

If an internal DNS server exists, there may also be a possibility to do a zone transfer from the internet to the internal DNS server. This may reveal information on IP address structure and naming structure

within the company to unauthorized users on the outside.
Only UDP based DNS queries should be enabled from the internal DNS server to the Internet.
By using a 'caching only' DNS server internally, and leaving the primary and secondary DNS information for the GM.xx domain at the external ISP's DNS servers, security for DNS is properly maintained.

Protecting the Firewall-1 system

Most firewall systems are heavily protected against attacks from external connections. However many companies fail to protect the firewall itself from internal users/hosts, making the firewall open to DoS (Denial-of-Service) attacks. These attacks may stop the firewall for a shorter period of time.
The rule base should start with these rules:
Rules that apply to the management of Firewall-1 (FW-1 control connections) – if there is to be no remote management then this rule should not exist.
One rule that denies all access to the firewall, regardless of source, service and time. This rule should have 'Action' set to 'Drop', and 'Track' set to 'Alarm'.

Last rule in the rule base

By default, the rule 'any – any – any- drop' applies to Firewall-1. This means that 'if no rule has accept-ed the packet, the packet will not be accepted'. This works the way it is supposed to be (except for those areas mentioned in chapter 4.1), but there is no logging or alarms. This is a severe security weak-ness, since there will exist no logfiles to prove unauthorised access or attempts to misuse the system.
The last rule in the rulebase should always be:
'Any – Any – Any – Drop – Log' as a minimum.

Anti-spoofing and use of IP addresses

Anti-spoofing is configured in the Firewall-1 object properties under the 'manage network objects' menu. Anti-spoofing is important to implement, otherwise it may be possible to send non-authorised packets through Firewall-1.
For the best protection, private IP addresses should be used internally, official IP addresses should be used for publicly available hosts in DMZ zones, and on the external connections.
Private IP addresses are defined in RFC's on the Internet, and defines these addresses for internal usage:
Class A: 10.0.0.0 – 10.255.255.255 subnet mask 255.0.0.0
Class B: 172.16.0.0 – 172.31.255.255 subnet mask 255.255.0.0
Class C: 192.168.0.0 – 192.168.255.255 subnet mask 255.255.255.0
In many cases this can not be done due to different reasons (both administrative and technical). In such cases it will be especially important to configure the anti-spoofing options correctly, and set off alarms on any attempt where spoofed packets are being received.

Using alternative domain names to hide the true identity when using services like WWW and FTP

Most companies allow their internal users to access the World Wide Web. At the same time they tell their users of the fact that the company's name (domain name) will be in the logs of each and every

site they visit. This may hurt the company's public image, if their domain name gets associated with sites containing controversial material like racism, pornography etc.
We recommend using this type of hiding the true identity, especially those accessing the Internet through the RAS services provided by the GM site.
By using multiple IP addresses, internal proxy servers and HIDE IP address translation for the proxy servers, the company may register one or more alternative domain names and use them to 'hide' their internal webusers behind alternative domain names.
As an example:
All mail will be sent out on the Internet from the domain GM.xx
All FTP and WWW traffic will come from STRANGEDOMAIN.NET, which is registered on Company XXX, or eventually a smaller subsidiary.
The alternative domain may easily be traced to GM.xx for security reasons, but log files on websites will only know of STRANGEDOMAIN.NET.

Differences in using 'Drop' and 'Reject' in the 'Action' setting for each rule

Under the 'Action' field in the Rule Base there exists two options for stopping packets. Although both options does stop the packet from going through the firewall, there is an important difference between these two options.
- REJECT will stop the packet, and send a message back to the sender that the packet was not ac-cepted.
- DROP does what it says; it drops the packet, but no message will be sent back to the sender.
DROP is the recommended setting.
REJECT may reveal the firewalls existence, and when a portscanning is done towards the firewall or any of its protected objects, the firewall will inform the portscanner which ports are not available on the target system. This is considered a severe security risk.
By using DROP the sender will not get any reply for those ports that are scanned. However, open ports will reply.
All ports that are open to the internet should normally be ports that 'everyone' are allowed to access. To get a complete list of open ports, open a DOS prompt and run the command 'netstat'. All listening and currently open ports will be shown.
REJECT may be used under certain conditions:
If internal users are accessing SMTP/POP3 accounts on external systems (their private mailboxes with an ISP), the remote mailserver may attempt to do and IDENT request back to the firewall. This request is initiated from the server, and will cause the connection to 'hang' for up to 30 seconds, since the pack-et is dropped by the firewall. By inserting a rule that specifically REJECTS Identd requests from the external mailserver, this can be avoided.

Unnecessary services should be removed.

These include ALL services that allow some kind of remote operation/control of the Windows NT con-figuration. If possible, the Firewall-1 systems should be moved within reasonable physical distance for the Firewall-1 administrators.
It should be impossible to do any type of administration of the Windows NT system remotely, only Fire-wall-1 administration. All administrative work that needs to be done at the computer should be per-formed by logging in to the local console.

Risk of losing log data, or log data being manipulated.

Even if log data are being fetched remotely from the Firewall-1, it is important that all log data are also being saved safely on the firewall system. We recommend using WORM drives (Write Once Read Many) for backup of log files frequently.
We also recommend having a local printer attached to each firewall, for the purpose of directly printing log information as evidence, if necessary.
Log data that are being sent/fetched from the firewall by any other system should also be stored at se-cure systems/media, such as WORM drives.

The Firewall Hardening Guide v0.1 - Checkpoint Firewall-1 Specific Requirements

Implicit Rules (Rule Zero rules)

DNS Rule Zero Rules

Open the Properties Setup window. Deselect both “Accept Domain Name Queries” checkboxs (UDP & TCP).
Insert specific rules to manage the DNS traffic. Rule Zero Rules are rules that get executed before any user defined rule. They Do Not appear in the normal rule table, but appear in a configuration screen. The DNS Rules are risky because the default configuration allows traffic on the DNS port to traverse the firewall without being controlled from any port. This rule has been used to enable such tools as BackOrifice to bypass the firewall.
Insert specific rules to manage the DNS traffic. Rule Zero Rules are rules that get executed before any user defined rule. They Do Not appear in the normal rule table, but appear in a configuration screen. The DNS Rules are risky because the default configuration allows traffic on the DNS port to traverse the firewall without being controlled from any port. This rule has been used to enable such tools as BackOrifice to bypass the firewall.

FW-1 Control Connections

FW-1 accepts connections on any of the Firewall-1 management ports. These include:
TCP port 256 - 259 and 261
UDP port 161 (SNMP)
TCP port 18181 – 18184
IP Type=94 (IP within IP encapsulation)
This setting should be disabled in control properties, and enabled through the rule base. This is done to be able to log, and also gain better control of traffic on this port.

Apply gateway rules to interface direction

The communication direction in which rules that are installed on gateways will be enforced. A setting of ‘Inbound’ applies the policy rules to traffic as it enters the firewall. ‘Outbound’ applies the policy rules after the firewall receives the traffic while ‘Eitherbound’ applies the rules in both directions. Eitherbound can cause traffic to be processed twice by the rule base.
Our recommendation is to use ‘Inbound’.
This will check the data as they enter the firewall. Eitherbound will represent a doubling in processing

load, and is not recommended.

TCP session timeout

This parameter is by default set to 3600 seconds (1 hour), the time period which a TCP session will be considered to have timed out. This is useful for protocols such as FTP which can be inactive for a long period (the FTP control session does not use keep-alives while the data session is transferring information).
Default 3600 seconds is recommended
By lowering this value users will experience more problems with broken connections in their sessions. On the other hand a higher value increases the risk of session hijacking and programs like trojan hors-es to operate undetected.

Accept UDP Replies

A UDP service sets up a two-way communication between the source and the destination; that is, when the communication is established between the source and the destination, a reply channel is also cre-ated between the destination and the source. When a UDP service communication is accepted on the destination and Enable UDP Replies is active, the reply channel is allowed. Only packets from the des-tination host and port are accepted as part of this communication.
This setting should be enabled.

Reply Timeout

The amount of time a UDP reply channel may remain open without any packets being returned. Since the communication is connectionless, there is no way to inform the reply channel when the communi-cation has finished. Note that FireWall-1 creates a connection context for UDP. Once the specified time has elapsed, the session is assumed to have ended and the reply channel is closed.
The default value is normally to be secure.

Accept Outgoing Packets

Allow all traffic originating from the firewall. This may be required if the rules have been applied Either-bound, NAT is being performed, or you are using security servers (i.e. FW-1 proxies).
This setting should be enabled. Otherwise no traffic will ever leave the firewall in any direction, making the firewall act as a ‘black hole’.

Enable Decryption on Accept

Decrypt incoming packets even if the rule accepting the connection does not specify it.
This setting should be enabled.

Use Fastpath/Fastmode

(This option is no longer available in V4.xx, but may be defined for TCP services that does not require encryption or authentication. The option is renamed Fastmode)The Fastpath feature speeds the process of forwarding traffic but does so at the cost of security.
Use Fastpath should be disabled. If Fastpath is enabled, encryption and authentication cannot be used. The firewall will also be less picky in inspecting passing traffic. Using fastmode for TCP services in

general is not recommended, unless one or more of the following conditions apply:

Synchronisation between firewalls are being used

Packet loss can be documented (Fastmode will speed up the processing of TCP packets). In normal installations packet loss should not occur until throughput exceeds 30 – 60 Mbit. (ref. CheckPoint documentation on performance for Firewall-1 under various operating systems.)

Accept RIP

Accept Routing Information Protocol traffic used for dynamic routing. RIP maintains information about reachable systems and routes to those systems. This setting assumes that RIP is running on the fire-wall. You should always use static route entries on a firewall unless you are running redundant firewalls or Internet links.
This setting should be disabled, unless RIP Must used through the Firewall-1 (not recommended).

Accept ICMP

Allow all ICMP based traffic.
Each of these rules are processed based on the pull down setting to the right. The options are:
First: Accept this traffic before processing the rule base.
Before Last: Accept this traffic, unless the rule base specifically blocks it from taking place.
Last: Process this traffic after the last rule in the rule base. If it is not specifically blocked, let it pass. If the last rule is "Drop all traffic from any source to any destination," this property is not evaluat-ed.
There are 17 types of ICMP, where types like ‘host unreachable’ and ‘source quench’ represent secu-rity risks for DoS (Denial-of-Service) attacks. Normally there should be no need for ICMP through the firewall. RFC 1700 holds more information on ICMP.
This setting should be disabled. ICMP passing through the firewall will not be needed under nor-mal circumstances, and will only serve as a security risk.