NIST Special Publication 800-XX

IMPLEMENTING INTERNET FIREWALL SECURITY POLICY

Barbara Guttman
Robert Bagwill

Information Technology Laboratory
Computer Security Division

National Institute of Standards and

U.S. Department of Commerce
William M. Daley, Secretary

Technology Administration
Gary R. Bachula, Acting Under Secretary for Technology

National Institute of Standards and Technology
Raymond Kammer, Director

1 Background and Purpose

Many organizations have connected or want to connect their private LAN's to the Internet so that their users can have convenient access to Internet services. Since the Internet as a whole is not trustworthy, their private systems are vulnerable to misuse and attack. A *firewall* is a safeguard one can use to control access between a trusted network and a less trusted one. A firewall is not a single component, it is a strategy for protecting an organization's Internet-reachable resources. Firewalls can also be used to secure segments of an organization's *intranet*, but this document will concentrate on the Internet aspects of firewall policy.

A firewall enforces a security policy, so without a policy, a firewall is useless. This document will help the responsible manager and firewall administrator create useful policy for the firewall. Throughout this document the term *firewall* refers to the sum of the hardware, software, policy and procedures used to implement the firewall policy. A firewall is not necessarily a single piece of software sitting on a single computer system,

For more information on firewalls, see NIST Special Publication 800-10 *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*.

2 Overview

The main function of a firewall is to centralize access control. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks. If outsiders or remote users can access the internal networks without going through the firewall, its effectiveness is diluted. For example, if a traveling manager has a modem connected to his office PC that he or she can dial into while traveling, and that PC is also on the protected internal network, an attacker who can dial into that PC has circumvented the firewall. Similarly, if a user has a dial-up Internet account with a commercial ISP, and sometimes connects to the Internet from their office PC via modem, he or she is opening an unsecured connection to the Internet that circumvents the firewall.

Firewalls provide several types of protection:

- They can block unwanted traffic.
- They can direct incoming traffic to more trustworthy internal systems.
- They hide vulnerable systems which can't easily be secured from the Internet.
- They can log traffic to and from the private network.
- They can hide information like system names, network topology, network device types, and internal user ID's from the Internet.
- They can provide more robust authentication than standard applications might be able to do.

Each of these functions are described in more detail below.

As with any safeguard, there are trade-offs between convenience and security. Transparency is the visibility of the firewall to both inside users and outsiders going through a firewall. A firewall is transparent to users if they do not notice or stop at the firewall in order to access a network. Firewalls are typically configured to be transparent to internal network users (while going outside the firewall); on the other hand, firewalls are configured to be non-transparent for outside network coming through the firewall. This generally provides the highest level of security without placing an undue burden on internal users.

3 Firewall Architectures

Firewalls can be configured in a number of different architectures, provided various levels of security at different costs of installation and operation. Organizations should match their risk

transparent. Filtering rules are not often easily maintained on a router, but there are tools available to simplify the tasks of creating and maintaining the rules.

Low Risk

5 Issues

5.1 Authentication

Router-based firewalls don't provide user authentication. Host-based firewalls can provide these kinds of authentication:

Username/password This provides the lowest level of protection, because the information can be sniffed off the network or shoulder-surfed.

One-time passwords One-time passwords using software or hardware tokens, generate a new password for each session. This means that old passwords cannot be reused if they are sniffed or otherwise borrowed or stolen.

Digital Certificates Digital certificates use a certificate generated using public key encryption.

5.2 Routing Versus Forwarding

A clearly defined policy has to be written as to whether or not the firewall will act as a router or a forwarder of Internet packets. This is trivial in the case of a router that acts as a packet filtering gateway: the firewall (router in this case) has no option but to route packets. Applications gateway firewalls should generally not be configured to route any traffic between the external interface and the internal network interface, since this could bypass security controls. All external to internal connections should go through the application proxies.

5.3 Source Routing

Source routing is a routing mechanism whereby the path to a target machine is determined by the source, rather than by intermediate routers. Source routing is mostly used for debugging network problems but could also be used to attack a host. If an attacker has knowledge of some trust relationship between your hosts, source routing can be used to make it appear that the malicious packets are coming from a trusted host. Therefore, because of this security threat, a packet filtering router can easily be configured to reject packets containing source route option. Thus a site that wishes to avoid the problem of source routing entirely would write a policy similar to the following:

5.4 IP Spoofing

IP spoofing is when an attacker masquerades his machine as a host on the target's network (i.e. fooling a target machine that packets are coming from a trusted machine on the target's internal network). Policy regarding packet routing has to be clearly written so that they will be handled accordingly if there is a security problem. It is necessary that authentication based on source address be combined with other security scheme to protect against IP spoofing attacks.

5.5 DNS and Mail Resolution

On the Internet, the Domain Name Service provides the mapping and translation of domain names to IP addresses, such as mapping server1.acme.com to 123.45.67.8. Some firewalls can be configured to run as a primary, secondary, or caching DNS server.

Deciding how to manage DNS services is generally not a security decision. Many organizations use a third party, such as an Internet Service Provider, to manage their DNS. In this case, the firewall can be used as a DNS caching server, improving performance but not requiring your organization to maintain its own DNS database.

If the organization decides to manage its own DNS database, the firewall can (but doesn't have to) act as the DNS server. If the firewall is to be configured as a DNS server (primary,

secondary, or caching), it is necessary that other security precautions be in place. One advantage of implementing the firewall as a DNS server is that it can be configured to hide the

High

All connections from the ORGANIZATION network to external networks must be approved by and managed by the Network Services Manager. Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures. All connections to approved external networks will pass through

9.1 Qualification of the Firewall Administrator

Two experienced people are generally recommended for the day to day administration of the firewall. In this manner availability of the firewall administrative function is largely insured. It should be required that information about each firewall administrator be written down so that he may contacting is possible in the event of a problem.

Security of a site is crucial to the day to day business activity of an organization. It is therefore required that the administrator of the firewall have a sound understanding of network concepts and implementation. For instance, since most firewalls are TCP/IP based, a thorough understanding of this protocol is compulsory. (Also see sections 9, LAN Administration and 5.7., Awareness and Education, for more information on the knowledge base required of technical administrative roles.)

An individual that is assigned the task of firewall administration must have a good hands-on experience with networking concepts, design, and implementation so that the firewall is configured correctly and administered properly. Firewall administrators should receive periodic training on the firewalls in use and in network security principals and practices.

9.2 Remote Firewall Administration

Firewalls are the first line of defense visible to an attacker. By design, firewalls are generally difficult to attack directly, causing attackers to often target the administrative accounts on a firewall. The username/password of administrative accounts must be strongly protected.

The most secure method of protecting against this form of attack is to have strong physical security around the firewall host and to only allow firewall administration from an attached terminal. However, operational concerns often dictate that some form of remote access for firewall administration be supported. In no case should remote access to the firewall be supported over untrusted networks without some form of strong authentication. In addition, to prevent eavesdropping, session encryption should be used for remote firewall connections.

Low

Any remote access over untrusted networks to the firewall for administration must use strong authentication, such as one time passwords and/or hardware tokens.

Medium

The preferred method for firewall administration is directly from the attached terminal. Physical access to the firewall terminal is limited to the firewall administrator and backup administrator.

Where remote access for firewall administration must be allowed, it should be limited to access from other hosts on the ORGANIZATION internal network. Such internal remote access requires the use of strong authentication, such as one time passwords and/or hardware tokens. Remote access over untrusted networks such as the Internet requires end to end encryption and strong authentication to be employed.

High

All firewall administration must be performed from the local terminal - no access to the firewall operating software is permitted via remote access. Physical access to the firewall terminal is limited to the firewall administrator and backup administrator.

9.3 User Accounts

Firewalls should never be used as general purpose servers. The only user accounts on the firewall should be those of the firewall administrator and any backup administrators. In addition, only these administrators should have privileges for updating system executables or other system software.

Only the firewall administrator and backup administrators will be given user accounts on the ORGANIZATION firewall. Any modification of the firewall system software must be done by the firewall administrator or backup administrator and requires approval of the Network Services Manager

9.4 Firewall Backup

To support recovery after failure or natural disaster, a firewall like any other network host has to have some policy defining system backup. Data files as well as system configuration files need to be have some backup plan in case of firewall failure.

The firewall (system software, configuration data, database files, etc.) must be backed up daily, weekly, and monthly so that in case of system failure, data and configuration files can be recovered. Backup files should be stored securely on a read-only media so that data in storage is not over-written inadvertently and locked up so that the media is only accessible to the appropriate personnel.

Another backup alternative would be to have another firewall configured as one already deployed and kept safely so that in case there is a failure of the current one, this backup firewall would simply be turned on and used as the firewall while the previous is undergoing a repair.

At least one firewall shall be configured and reserved (not-in-use) so that in case of a firewall failure, this backup firewall can be switched in to protect the network.

9.5 System Integrity

To prevent unauthorized modifications of the firewall configuration, some form of integrity assurance process should be used. Typically, checksums, cyclic redundancy checks, or cryptographic hashes are made from the runtime image and saved on protected media. Each time the firewall configuration has been modified by an authorized individual (usually the firewall administrator), it is necessary that the system integrity online database be updated and saved onto a file system on the network or removable media. If the system integrity check shows that the firewall configuration files have been modified, it will be known that the system has been compromised.

The firewall's system integrity database shall be updated each time the firewall is configuration is modified. System integrity files must be stored on read only media or off-line storage. System integrity shall be checked on a regular basis on the firewall in order for the administrator to generate a listing of all files that may have been modified, replaced, or deleted.

9.6 Documentation

It is important that the operational procedures for a firewall and its configurable parameters be well documented, updated, and kept in a safe and secure place. This assures that if a firewall administrator resigns or is otherwise unavailable, an experienced individual can read the documentation and rapidly pick up the administration of the firewall. In the event of a break-in such documentation also supports trying to recreate the events that caused the security incident.

9.7 Physical Firewall Security

Physical access to the firewall must be tightly controlled to preclude any authorized changes to the firewall configuration or operational status, and to eliminate any potential for monitoring firewall activity. In addition, precautions should be taken to assure that proper environment alarms and backup systems are available to assure the firewall remains online.

The ORGANIZATION firewall should be located in an controlled environment, with access limited to the Network Services Manager, the firewall administrator, and the backup firewall administrator.

The room in which the firewall is to be physically located must be equipped with heat, air-conditioner, and smoke alarms to assure the proper working order of the room. The placement and recharge status of the fire extinguishers shall be checked on a regular basis. If uninterruptible power service is available to any Internet-connected systems, such service should be provided to the firewall as well.

9.8 Firewall Incident Handling

Incident reporting is the process whereby certain anomalies are reported or logged on the firewall. A policy is required to determine what type of report to log and what to do with the generated log report. This should be consistent with Incident Handling policies detailed in section 5.5. The following policies are appropriate to all risk environments.

The firewall shall be configured to log all reports on daily, weekly, and monthly bases so that the network activity can be analyzed when needed.

Firewall logs should be examined on a weekly basis to determine if attacks have been detected.

The firewall administrator shall be notified at anytime of any security alarm by email, pager, or other means so that he may immediately respond to such alarm.

The firewall shall reject any kind of probing or scanning tool that is directed to it so that information being protected is not leaked out by the firewall. In a similar fashion, the firewall shall block all software types that are known to present security threats to a network (such as Active X and Java) to better tighten the security of the network.

9.9 Restoration of Services

Once an incident has been detected, the firewall may need to be brought down and reconfigured. If it is necessary to bring down the firewall, Internet service should be disabled or a secondary firewall should be made operational - internal systems should not be connected to the Internet without a firewall. After being reconfigured, the firewall must be brought back into an operational and reliable state. Policies for restoring the firewall to a working state when a break-in occurs are needed.

In case of a firewall break-in, the firewall administrator(s) are responsible for reconfiguring the firewall to address any vulnerabilities that were exploited. The firewall shall be restored to the state it was before the break-in so that the network is not left wide open. While the restoration is going on, the backup firewall shall be deployed.

9.10 Upgrading the firewall

It is often necessary that the firewall software and hardware components be upgraded with the necessary modules to assure optimal firewall performance. The firewall administrator should be aware of any hardware and software bugs, as well as firewall software upgrades that may be issued by the vendor. If an upgrade of any sort is necessary, certain precautions must be taken

to continue to maintain a high level of operational security. Sample policies that should be written for upgrades may include:

To optimize the performance of the firewall, all vendor recommendations for processor and memory capacities shall be followed.

The firewall administrator must evaluate each new release of the firewall software to determine if an upgrade is required. All security patches recommended by the firewall vendor should be implemented in a timely manner.

Hardware and software components shall be obtained from a list of vendor-recommended sources. Any firewall specific upgrades shall be obtained from the vendor. NFS shall not be used as a means of obtaining hardware and software components. The use of virus checked CDROM or FTP to a vendor's site is an appropriate method.

The firewall administrator(s) shall monitor the vendor's firewall mailing list or maintain some other form of contact with the vendor to be aware of all required upgrades. Before an upgrade of any of the firewall component, the firewall administrator must verify with the vendor that an upgrade is required. After any upgrade the firewall shall be tested to verify proper operation prior to going operational.

9.11 Logs and Audit Trails (Audit/Event Reporting and Summaries)

Most firewalls provide a wide range of capabilities for logging traffic and network events. Some security-relevant event that should be recorded on the firewall's audit trail logs are: hardware and disk media errors, login/logout activity, connect time, use of system administrator privileges, inbound and outbound e-mail traffic, TCP network connect attempts, in-bound and out-bound proxy traffic type.

10 Revision/Update of Firewall Policy

Given the rapid introduction of new technologies, and the tendency for organizations to continually introduce new services, firewall security policies should be reviewed on a regular basis. As network requirements changes, so should security policy.

11 Example General Policies

The following policy statements are only examples. They do not constitute a complete firewall policy, and even if they did, they would not necessarily apply to your organization's environment.

Manager

A firewall shall be placed between the ORGANIZATION's network and the Internet to prevent untrusted networks from accessing the ORGANIZATION network. The firewall will be selected by and maintained by the Network Services Manager.

All other forms of Internet access (such as via dial-out modems) from sites connected to the ORGANIZATION wide-area network are prohibited.

All users who require access to Internet services must do so by using ORGANIZATION-approved software and Internet gateways.

Technician

All firewalls should fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a failure.

Source routing shall be disabled on all firewalls and external routers (see section 5.3).

The firewall shall not accept traffic on its external interfaces that appear to be coming from internal network addresses (see section 5.4).

The firewall shall provide detailed audit logs of all sessions so that these logs can be reviewed for any anomalies.

Secure media shall be used to store log reports such that access to this media is restricted to only authorized personnel.

Firewalls shall be tested off-line and the proper configuration verified.

The firewall shall be configured to implement transparency for all outbound services. Unless approved by the Network Services manager, all in-bound services shall be intercepted and processed by the firewall.

Appropriate firewall documentation will be maintained on off-line storage at all times. Such information shall include but not be limited to the network diagram, including all IP addresses of all network devices, the IP addresses of relevant hosts of the Internet Service Provider (ISP) such as external news server, router, DNS server, etc. and all other configuration parameters such as packet filter rules, etc. Such documentation shall be updated any time the firewall configuration is changed.

Medium-Risk Environment Policies

User

When you are off-site, you may only access internal systems by using ORGANIZATION-approved one-time passwords and hardware tokens to authenticate yourself to the firewall. Any other means of accessing internal systems is prohibited.

Manager

Strong authentication using ORGANIZATION-approved one-time passwords and hardware tokens is required all remote access to internal systems through the firewall.

The network security policy shall be reviewed on a regular basis (every three months minimum) by the firewall administrator(s) and other top information (security) managers. Where requirements for network connections and services have changed, the security policy shall be updated and approved. If a change is to be made, the firewall administrator shall ensure that the change is implemented and the policy modified.

The details of the ORGANIZATION internal trusted network should not be visible from outside the firewall.

Technician

The firewall will be configured to deny all services not expressly permitted and will be regularly audited and monitored to detect intrusions or misuse.

The firewall shall notify the system administrator in near-real-time of any item that may need immediate attention such as a break-in into the network, little disk space available, or other related messages so that an immediate action could be taken.

The firewall software will run on a dedicated computer - all non-firewall related software, such as compilers, editors, communications software, etc., will be deleted or disabled.

The firewall will be configured to deny all services not expressly permitted and will be regularly audited and monitored to detect intrusions or misuse.

High-Risk Environment Policies

User

All non-business use of the Internet from ORGANIZATION systems is forbidden. All access to Internet services is logged. Employees who violate this policy are subject to disciplinary action.

Your browser has been configured with a list of forbidden sites. Any attempts to access those sites will be reported to your manager.

Manager

All non-business use of the Internet from ORGANIZATION systems is forbidden. All access to Internet services is logged. Employees who violate this policy are subject to disciplinary action.

Technician

All access to Internet services is logged. Summary and exception reports will be prepared for the network and security managers.

12 Example Service-Specific Policies

Connecting to the Internet makes a wide range of services available to internal users and a wide range of system accesses available to external users. Driven by the needs of the business or mission side of the organization, policy has to be clearly written to state what services to allow or disallow to both inside and outside networks.

There is a wide range of Internet services available. Section 4 discusses the most popular services, such as FTP, telnet, HTTP, etc. Other common services are detailed here.

Berkeley Software Distribution (BSD) UNIX “r” commands, such as rsh, rlogin, rcp, etc., are designed to allow UNIX system users to execute commands on remote systems. Most implementation do not support authentication or encryption and are very dangerous to use over the Internet.

Post Office Protocol (POP) is a client-server protocol for retrieving electronic mail from a server. POP is a TCP-based service that supports the use of nonreusable passwords for authentication, known as APOP. POP does not support encryption - retrieved email is vulnerable to eavesdropping.

Network News Transfer Protocol (NNTP) is used to support Usenet newsgroups. NNTP is a TCP-based service that implements a store and forward protocol. While NNTP is a relatively simple protocol, there have been recent attacks against common NNTP server software. NNTP servers should not be run on the firewall, but standard proxy services are available to pass NNTP.

Finger and whois are similar functions. finger is used to retrieve information about system users. finger often gives out more information than is necessary - for most organizations finger should be disabled or limited at the firewall. Whois is very similar and should also be disabled or limited at the firewall.

The UNIX remote printing protocols lp and lpr allow remote hosts to print using printers attached to other hosts. Lpr is a store and forward protocol, while lp uses the rsh function to provide remote printing capabilities. In general, lp and lpr should be disabled at the firewall unless vendor supplied proxies are available.

Network File System (NFS) allows disk drives to be made accessible to users and systems across the network. NFS uses a very weak form of authentication and is not considered safe to use across untrusted networks. NFS should not be allowed through a firewall.

Real Audio provides for the delivery of digitized audio over TCP/IP networks. - To take advantage of the multimedia capabilities of the World Wide Web, a number of new services have been developed.

Which Internet services to allow or deny must be driven by the needs of the organization. Sample security policy for some of these Internet services that might be required by a typical organization are illustrated in Table 5.2.

- Status (Y/N) = whether users can use the service
- Auth (Y/N) = whether any form of authentication (strong or otherwise) is performed before the service can be used.

12.1 Manager

A table of the managerial-level concerns follows.

Table 2- Managerial Concerns

Purpose	Protocols	What	Why
Email		Users have a single external email address	• Does not reveal business info.
	SMTP	• A single server or cluster of servers provides email service for organization	• Centralized email is easier to maintain. • SMTP servers are difficult to configure securely.
	POP3	• POP users must use AUTH identification.	• Prevents password sniffing.
	IMAP	• Groups are encouraged to transition to IMAP.	• Better support for travel, encryption.
USENET news	NTTP	• blocked at firewall	• no business need

Purpose	Protocols	What	Why
WWW	HTTP	• directed to www.my.org	• Centralized WWW is easier to maintain. • WWW servers are difficult to configure securely.

finger	y	n	n	n	Inbound finger services are to be disabled at the ORGANIZATION firewall
gopher	y	n	n	n	Inbound gopher services are to be disabled at the ORGANIZATION firewall
whois	y	n	n	n	Inbound whois services are to be disabled at the ORGANIZATION firewall
SQL	y	n	n	n	Connections from external hosts to internal databases must be approved by the Network Services Manager and used approved SQL proxy services.
Rsh	y	n	n	n	Inbound rsh services are to be disabled at the