DATA SECURITY MANAGEMENT

SECURED CONNECTIONS TO EXTERNAL NETWORKS

Steven F. Blanding

INSIDE
Risks and Assumptions; Security Policies; Identification and Authentication; Static Authentication; Robust Authentication; Continuous Authentication; Applying Identification and Authorization Policies; Password Management Policies; Robust Authentication Policy

INTRODUCTION
A private network that carries sensitive data between local computers requires proper security measures to protect the privacy and integrity of the traffic. When such a network is connected to other networks, or when telephone access is allowed into that network, the remote terminals, phone lines, and other connections become extensions to that private network and must be secured accordingly. In addition, the private network must be secured from outside attacks that could cause loss of information, breakdowns in network integrity, or breaches in security.

Many organizations have connected or want to connect their private local area networks (LANs) to the Internet so that their users can have convenient access to Internet services. Since the Internet as a whole is not trustworthy, private systems are vulnerable to misuse and attack. Firewalls are typically used as a safeguard to control access between a trusted network and a less trusted network. A firewall is not a single component; it is a strategy for protecting an organization’s resources from the Internet. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks. Some organizations are also in the process of connecting their private networks to other organizations’ private networks. Firewall security capabilities should also be used to provide protection for these types of connections as well.

This article identifies areas of security that should be considered with connections to external networks. Security policies must be developed

PAYOFF IDEA
Private networks containing sensitive data must be protected against any compromise of privacy and integrity, from connections to external, untrusted networks. This article identifies those areas of security that must be considered when planning connections to external networks.
for user identification and authorization, software import controls, en-
cryption, and system architecture, which include the use of Internet fire-
wall security capabilities. This article discusses security policy statements
that address connections to external networks, including the Internet.
Each section contains multiple sample policies for use at the different risk
profiles. Some areas provide multiple examples at the same risk level to
show the different presentation methods that might be used to relay the
message.

This first section discusses the risks and assumptions that should be
acknowledged before a security analysis can be performed.

RISKS AND ASSUMPTIONS
An understanding of the risks and assumptions is required before defin-
ing security policies for external connections. It is beyond the scope of
this article to quantify the probability of the risks; however, the risks
should cover a broad, comprehensive area. The following are the risks
and assumptions.

• The data being protected, while not classified, is highly sensitive and
would do damage to the organization and its mission if disclosed or
captured.
• The integrity of the internal network directly affects the ability of the
organization to accomplish its mission.
• The internal network is physically secure; the people using the inter-
network are trustworthy.
• PCs on the internal network are considered to be unsecured. Reli-
ance is placed on the physical security of the location to protect
them.
• Whenever possible, employees who are connected from remote sites
should be treated as members of the internal network and have ac-
cess to as many services as is possible without compromising internal
security.
• The Internet is assumed to be unsecured; the people using the Inter-
et are assumed to be untrustworthy.
• Employees are targets for spying; information they carry or commu-
nicate is vulnerable to capture.
• Passwords transmitted over outside connections are vulnerable to
capture.
• Any data transmitted over outside connections is vulnerable to cap-
ture.
• There is no control over e-mail once it leaves the internal network; e-
mail can be read, tampered with, and spoofed.
• Any direct connection between a PC on the internal network and one
on the outside can possibly be compromised and used for intrusion.
• Software bugs exist and may provide intrusion points from the outside into the internal network.
• Password protection on PCs directly reachable from the outside can be compromised and used for intrusion.
• Security through obscurity is counterproductive. Easy-to-understand measures are more likely to be sound, and are easier to administer.

SECURITY POLICIES
Security policies fall into two broad categories: technical policies to be carried out by hardware or software, and administrative policy to be carried out by people using and managing the system. The final section of this article discusses Internet firewall security policies in more detail.

Identification and Authentication
Identification and authentication are the processes of recognizing and verifying valid users or processes. Identification and authentication information is generally used to determine what system resources a user or process will be allowed to access. The determination of who can access what should coincide with a data categorization effort.

The assumption is that there is connectivity to internal systems from external networks or the Internet. If there is no connectivity, there is no need for identification and authentication controls. Many organizations separate Internet-accessible systems from internal systems through the use of firewalls and routers.

Authentication over the Internet presents several problems. It is relatively easy to capture identification and authentication data (or any data) and replay it in order to impersonate a user. As with other remote identification and authorization controls, and often with internal authorization systems, there can be a high level of user dissatisfaction and uncertainty that can make this data obtainable via social engineering. Having additional authorization controls for use of the Internet may also contribute to authorization data proliferation, which is difficult for users to manage. Another problem is the ability to hijack a user session after the identification and authorization have been performed.

There are three major types of authentication available: static, robust, and continuous. Static authentication includes passwords and other techniques that can be compromised through replay attacks. They are often called reusable passwords. Robust authentication involves the use of cryptography or other techniques to create one-time passwords that are used to create sessions. These can be compromised by session hijacking. Continuous authentication prevents session hijacking.

Static Authentication. Static authentication only provides protection against attacks in which an imposter cannot see, insert, or alter the infor-
mation passed between the claimant and the verifier during an authenti-
cation exchange and subsequent session. In these cases, an imposter can
only attempt to assume a claimant's identity by initiating an access con-
trol session as any valid user might do and trying to guess a legitimate
user's authentication data. Traditional password schemes provide this
level of protection, and the strength of the authentication process is high-
ly dependent on the difficulty of guessing password values and how well
they are protected.

**Robust Authentication.** This class of authentication mechanisms relies
on dynamic authentication data that changes with each authenticated
session between a claimant and verifier. An imposter who can see infor-
mation passed between the claimant and verifier may attempt to record
this information, initiate a separate access control session with the verifi-
er, and replay the recorded authentication data in an attempt to assume
the claimant's identity. This type of authentication protects against such
attacks because authentication data recorded during a previous session
will not be valid for any subsequent sessions.

However, robust authentication does not provide protection against
active attacks in which the imposer is able to alter the content or flow of
information between the claimant and verifier after they have established
a legitimate session. Since the verifier binds the claimant's identity to the
logical communications channel for the duration of the session, the ver-
ifier believes that the claimant is the source of all data received through
this channel.

Traditional fixed passwords would fail to provide robust authentica-
tion because the password of a valid user could be viewed and used to
assume that user's identity later. However, one-time passwords and digi-
tal signatures can provide this level of protection.

**Continuous Authentication.** This type of authentication provides pro-
tection against impostors who can see, alter, and insert information
passed between the claimant and verifier even after the claimant/verifier
authentication is complete. These are typically referred to as active at-
tacks because they assume that the imposter can actively influence the
connection between claimant and verifier. One way to provide this form
of authentication is to apply a digital signature algorithm to every bit of
data that is sent from the claimant to the verifier. There are other combi-
nations of cryptography that can provide this form of authentication, but
current strategies rely on applying some type of cryptography to every
bit of data sent. Otherwise, any unprotected bit would be suspect.

*Applying Identification and Authorization Policies*

Although passwords are easily compromised, an organization may find
that a threat is not likely, would be fairly easy to recover from, or would
not affect critical systems (which may have separate protection mechanisms). In low-risk connections, only static authentication may be required for access to corporate systems from external networks or the Internet.

In medium-risk connections, Internet access to information and processing (low impact if modified, unavailable, or disclosed) would require a password, and access to all other resources would require robust authentication. Telnet access to corporate resources from the Internet would also require the use of robust authentication.

Internet access to all systems behind the firewall would require robust authentication. Access to information and processing (high impact if modified, unavailable, or disclosed) would require continuous authentication.

Password Management Policies
The following are general password policies applicable for Internet use. These are considered to be the minimum standards for security control.

- Passwords and user log-on IDs will be unique to each authorized user.
- Passwords will consist of a minimum of six alphanumeric characters (no common names or phrases). There should be computer-controlled lists of proscribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words, and standard names) to identify any password weaknesses.
- Passwords will be kept private (i.e., not shared, coded into programs, or written down).
- Passwords will be changed every 90 days (or less). Most operating systems can enforce password change with an automatic expiration date and prevent repeated or reused passwords.
- User accounts will be frozen after three failed log-on attempts. All erroneous password entries will be recorded in an audit log for later inspection and action, as necessary.
- Sessions will be suspended after 15 minutes (or other specified period) of inactivity and require the password to be reentered.
- Successful log-ons should display the date and time of the last log-on and log-off.
- Log-on IDs and passwords should be suspended after a specified period of non-use.
- For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data, etc.) for the failed user (to keep this user connected while personnel attempt to investigate the incoming connection).

Robust Authentication Policy
The decision to use robust authentication requires an understanding of the risks, the security gained, and the cost of user acceptance and admin-
istration. User acceptance will be dramatically improved if users are appropriately trained about robust authentication and how it is used.

There are many technologies available that provide robust authentication, including dynamic password generators, cryptography-based challenge/response tokens and software, and digital signatures and certificates. If digital signatures and certificates are used, another policy area is opened up: the security requirements for the certificates.

Users of robust authentication must receive training prior to use of the authentication mechanism. Employees are responsible for safe handling and storage of all company authentication devices. Authentication tokens should not be stored with a computer that will be used to access corporate systems. If an authentication device is lost or stolen, the loss must be immediately reported to security so that the device can be disabled.

**Digital Signatures and Certificates.** If identification and authorization makes use of digital signatures, then certificates are required. They can be issued by the organization or by a trusted third party. Commercial public key infrastructure (PKI) is emerging within the Internet community. Users can obtain certificates with various levels of assurance. For example, Level 1 certificates verify electronic mail addresses. This is done through the use of a personal information number that a user would supply when asked to register. This level of certificate may also provide a name as well as an electronic mail address; however, it may or may not be a genuine name (i.e., it could be an alias). Level 2 certificates verify a user’s name, address, social security number, and other information against a credit bureau database. Level 3 certificates are available to companies. This level of certificate provides photo identification (e.g., for their employees) to accompany the other items of information provided by a Level 2 certificate.

Once obtained, digital certificate information can be loaded into an electronic mail application or a Web browser application to be activated and provided whenever a Web site or another user requests it for the purposes of verifying the identity of the person with whom they are communicating. Trusted certificate authorities are required to administer such systems with strict controls, otherwise fraudulent certificates could easily be issued.

Many of the latest Web servers and Web browsers incorporate the use of digital certificates. Secure socket layer (SSL) is the technology used in most Web-based applications. SSL version 2.0 supports strong authentication of the Web server, while SSL 3.0 added client-side authentication. Once both sides are authenticated, the session is encrypted, providing protection against both eavesdropping and session hijacking. The digital certificates used are based on the X.509 standard and describe who issued the certificate, the validity period, and other information.
Oddly enough, passwords still play an important role even when using digital certificates. Since a digital certificate is stored on a computer, it can only be used to authenticate the computer, rather than the user, unless the user provides some other form of authentication to the computer. Passwords or passphrases are generally used; smart cards and other hardware tokens will be used in the future.

Any company’s systems making limited distribution data available over the Internet should use digital certificates to validate the identity of both the user and the server. Only company-approved certificate authorities should issue certificates. Certificates at the user end should be used in conjunction with standard technologies such as SSL to provide continuous authentication to eliminate the risk of session hijacking. Access to digital certificates stored on personal computers should be protected by passwords or passphrases. All policies for password management must be followed and enforced.

**Software Import Control**

Data on computers is rarely static. Mail arrives and is read. New applications are loaded from floppy, CD-ROM, or across a network. Web-based interactive software downloads executables that run on a computer. Each modification runs the risk of introducing viruses, damaging the configuration of the computer, or violating software-licensing agreements. Organizations need to protect themselves with different levels of control, depending on the vulnerability to these risks. Software import control provides an organization with several different security challenges:

- virus and Trojan horse prevention, detection, and removal
- controlling interactive software (Java, ActiveX)
- software licensing

Each challenge can be categorized according to the following criteria:

- control: who initiates the activity, and how easily can it be determined that software has been imported
- threat type: executable program, macro, applet, violation of licensing agreement
- cleansing action: scanning, refusal of service, control of permissions, auditing, deletion

When importing software onto a computer, one runs the risk of getting additional or different functionality than one bargained for. The importation may occur as a direct action, or as a hidden side effect, which is not readily visible. Examples of direct action are:
• File transfer: utilizing ftp to transfer a file to a computer
• Reading e-mail: causing a message that has been transferred to a computer to be read, or using a tool (e.g., Microsoft Word) to read an attachment
• Downloading software, from a floppy disk or over the network can spawn indirect action: examples include (1) reading a Web page that downloads a Java applet to one’s computer and (2) executing an application such as Microsoft Word, and opening a file infected with a Word macro virus.

**Virus Prevention, Detection, and Removal.** A virus is a self-replicating program spread from executables, boot records, and macros. Executable viruses modify a program to do something other than the original intent. After replicating itself into other programs, the virus may do little more than print an annoying message, or be as damaging as deleting all of the data on a disk. There are different levels of sophistication in how hard a virus may be to detect.

The most common “carrier” of viruses has been the floppy disk, since “sneaker net” was the most common means of transferring software between computers. As telephone-based bulletin boards became popular, viruses traveled more frequently via modem. The Internet provides yet another channel for virus infections, one that can often bypass traditional virus controls.

For organizations that allow downloading of software over the Internet (which can be via Internet e-mail attachments), virus scanning at the firewall can be an appropriate choice — but it does not eliminate the need for client and server-based virus scanning as well. For several years to come, viruses imported on floppy disks or infected vendor media will continue to be a major threat.

Simple viruses can be easily recognized by scanning for a signature of byte strings near the entry point of a program, once the virus has been identified. Polymorphic viruses modify themselves as they propagate, therefore have no signature, and can only be found (safely) by executing the program in a virtual processor environment. Boot record viruses modify the boot record such that the virus is executed when the system is booted.

Applications that support macros are at risk for macro viruses. Macro viruses are commands that are embedded in data. Vendor applications, such as Microsoft Word, Microsoft Excel, or printing standards such as Postscript are common targets. When the application opens the data file the infected macro virus is instantiated.

The security service policy for viruses has three aspects:

• prevention: policies that prevent the introduction of viruses into a computing environment
• detection: determination that an executable, boot record, or data file is contaminated with a virus
• removal: deletion of the virus from the infected computing system

There are various factors that are important in determining the level of security concern for virus infection of a computer. Viruses are most prevalent on DOS, Windows (3.x, 95), and NT operating systems. However, some UNIX viruses have been identified.

The frequency with which new applications or files are loaded onto the computer is proportional to the susceptibility of that computer to viruses. Configuration changes resulting from exposure to the Internet, exposure to mail, or receipt of files from external sources are more at risk for contamination.

The greater the value of the computer or data on the computer, the greater the concern should be for ensuring that virus policy as well as implementation procedures are in place. The cost of removal of the virus from the computing environment must be considered within one’s organization as well as from customers one may have infected. Cost may not always be identified as monetary; company reputation and other considerations are just as important.

It is important to note that viruses are normally introduced into a system by a voluntary act of a user (e.g., installation of an application, executing a file, etc.). Prevention policies can therefore focus on limiting the introduction of potentially infected software and files to a system. In a high-risk environment, virus-scanning efforts should be focused on when new software or files are introduced to maximize protection.

**Controlling Interactive Software.** A programming environment evolving as a result of Internet technology is interactive software, as exemplified by Java and ActiveX. In an interactive software environment, a user accesses a server across a network. The server downloads an application (applet) onto the user’s computer that is then executed. There have been various claims that when utilizing languages such as Java, it is impossible to introduce a virus because of restrictions within the scripting language for file system access and process control. However, security risks using Java and ActiveX have been documented.

Therefore, there are several assumptions of trust that a user must make before employing this technology:

• The server can be trusted to download trustworthy applets.
• The applet will execute in a limited environment, restricting disk reads and writes to functions that do not have security.
The applet can be scanned to determine if it is safe.
Scripts are interpreted, not precompiled.

**Firewall Policy**

Firewalls are critical to the success of secured connections to external networks as well as the Internet. The main function of a firewall is to centralize access control. 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 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 controls imposed by the firewall. If a user has a dial-up Internet account with a commercial Internet service provider (ISP), and sometimes connects to the Internet from his office PC via modem, he is opening an unsecured connection to the Internet that circumvents the firewall.

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.

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 that cannot 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 IDs from the Internet.
- They can provide more robust authentication than standard applications might be able to do.

Each of these functions is 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 nontransparent for outside network users coming through the firewall. This generally provides the highest level of security without placing an undue burden on internal users.

**Firewall Authentication**

Router-based firewalls do not provide user authentication. Host-based firewalls can provide various kinds of authentication. Username/pass-
word authentication is the least secure because the information can be sniffed or shoulder-surfed. One-time passwords use software or hardware tokens and generate a new password for each session. This means that old passwords cannot be reused if they are sniffed or otherwise borrowed or stolen. Finally, digital certificates use a certificate generated using public key encryption.

**Routing Versus Forwarding.** A clearly defined policy should 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 because 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 because this could bypass security controls. All external-to-internal connections should go through the application proxies.

**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 an organization’s hosts, source routing can be used to make it appear that the malicious packets are coming from a trusted host. Because of this security threat, a packet filtering router can easily be configured to reject packets containing source route option.

**IP Spoofing.** IP spoofing occurs 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). Policies regarding packet routing need 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 schemes to protect against IP spoofing attacks.

**Types of Firewalls**
There are different implementations of firewalls, which can be arranged in different ways. These include packet filtering gateways, application gateways, and hybrid or complex gateways.

**Packet Filtering Gateways.** Packet filtering firewalls use routers with packet filtering rules to grant or deny access based on source address, destination address, and port. They offer minimum security but at a very low cost, and can be an appropriate choice for a low-risk environment.
They are fast, flexible, and 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.

Filtering gateways do have inherent risks, including:

- The source and destination addresses and ports contained in the IP packet header are the only information available to the router in making a decision whether or not to permit traffic access to an internal network.
- They do not protect against IP or DNS address spoofing.
- An attacker will have direct access to any host on the internal network once access has been granted by the firewall.
- Strong user authentication is not supported with packet filtering gateways.
- They provide little or no useful logging.

**Application Gateways.** An application gateway uses server programs called proxies that run on the firewall. These proxies take external requests, examine them, and forward legitimate requests to the internal host that provides the appropriate service. Application gateways can support functions such as user authentication and logging.

Because an application gateway is considered the most secure type of firewall, this configuration provides a number of advantages to the medium-high risk site:

- The firewall can be configured as the only host address that is visible to the outside network, thus requiring all connections to and from the internal network to go through the firewall.
- The use of proxies for different services prevents direct access to services on the internal network, thereby protecting the enterprise against insecure or misconfigured internal hosts.
- Strong user authentication can be enforced with application gateways.
- Proxies can provide detailed logging at the application level. Application-level firewalls are configured such that outbound network traffic appears as if the traffic had originated from the firewall (i.e., only the firewall is visible to outside networks). In this manner, direct access to network services on the internal network is not allowed. All incoming requests for different network services such as telnet, FTP, HTTP, RLOGIN, etc., regardless of which host on the internal network will be the final destination, must go through the appropriate proxy on the firewall.

Application gateways require a proxy for each service, such as FTP, HTTP, etc., to be supported through the firewall. When a service is re-
quired that is not supported by a proxy, an organization has three choices:

1. Deny the service until the firewall vendor has developed a secure proxy. This is the preferred approach, as many newly introduced Internet services have unacceptable vulnerabilities.
2. Develop a custom proxy. This is a fairly difficult task and should be undertaken only by very sophisticated technical organizations.
3. Pass the service through the firewall. Using what are typically called “plugs,” most application gateway firewalls allow services to be passed directly through the firewall with only a minimum of packet filtering. This can limit some of the vulnerability but can result in compromising the security of systems behind the firewall.

Hybrid or Complex Gateways. Hybrid gateways combine two or more of the above firewall types and implement them in series rather than in parallel. If they are connected in series, then the overall security is enhanced; on the other hand, if they are connected in parallel, then the network security perimeter will be only as secure as the least secure of all methods used. In medium- to high-risk environments, a hybrid gateway may be the ideal firewall implementation.

Suggested ratings are identified in Exhibit 1 for various firewall types.

Firewall Architectures

Firewalls can be configured in a number of different architectures, providing various levels of security at different costs of installation and operation. Organizations should match their risk profile to the type of firewall architecture selected. The following describes typical firewall architectures and sample policy statements.

Multi-Homed Host. A multi-homed host is a host (a firewall in this case) that has more than one network interface, with each interface connected to logically and physically separate network segments. A dual-homed host (host with two interfaces) is the most common instance of a multi-homed host.

EXHIBIT 1 — Firewall Security Risk

<table>
<thead>
<tr>
<th>Firewall Architecture</th>
<th>High-Risk Environment (e.g., hospital)</th>
<th>Medium-Risk Environment (e.g., university)</th>
<th>Low-Risk Environment (e.g., florist shop)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet filtering</td>
<td>Unacceptable</td>
<td>Minimal security</td>
<td>Recommended</td>
</tr>
<tr>
<td>Application gateways</td>
<td>Effective option</td>
<td>Recommended</td>
<td>Acceptable</td>
</tr>
<tr>
<td>Hybrid gateways</td>
<td>Recommended</td>
<td>Effective option</td>
<td>Acceptable</td>
</tr>
</tbody>
</table>
A dual-homed firewall is a firewall with two network interface cards (NICs) with each interface connected to different networks. For example, one network interface is typically connected to the external or untrusted network, while the other interface is connected to the internal or trusted network. In this configuration, a key security tenet is not to allow traffic coming in from the untrusted network to be directly routed to the trusted network; that is, the firewall must always act as an intermediary. Routing by the firewall must be disabled for a dual-homed firewall so that IP packets from one network are not directly routed from one network to the other.

Screened Host. A screened host firewall architecture uses a host (called a bastion host) to which all outside hosts connect, rather than allow direct connection to other, less secure internal hosts. To achieve this, a filtering router is configured so that all connections to the internal network from the outside network are directed toward the bastion host. If a packet filtering gateway is to be deployed, then a bastion host should be set up so that all connections from the outside network go through the bastion host to prevent direct Internet connection between the internal network and the outside world.

Screened Subnet. The screened subnet architecture is essentially the same as the screened host architecture, but adds an extra stratum of security by creating a network in which the bastion host resides (often called perimeter network) and which is separated from the internal network. A screened subnet is deployed by adding a perimeter network in order to separate the internal network from the external. This ensures that if there is a successful attack on the bastion host, the attacker is restricted to the perimeter network by the screening router that is connected between the internal and perimeter networks.

Intranet. Although firewalls are usually placed between a network and the outside untrusted network, in large companies or organizations, firewalls are often used to create different subnets of the network, often called an intranet. Intranet firewalls are intended to isolate a particular subnet from the overall corporate network. The reason for the isolation of a network segment might be that certain employees can only access subnets guarded by these firewalls only on a need-to-know basis. An example could be a firewall for the payroll or accounting department of an organization.

The decision to use an intranet firewall is generally based on the need to make certain information available to some but not all internal users, or to provide a high degree of accountability for the access and use of confidential or sensitive information.
For any systems hosting internal critical applications, or providing access to sensitive or confidential information, internal firewalls or filtering routers should be used to provide strong access control and support for auditing and logging. These controls should be used to segment the internal network to support the access policies developed by the designated owners of information.

Firewall Administration

A firewall — like any other network device — has to be managed by someone. Security policy should state who is responsible for managing the firewall.

Two firewall administrators (one primary and one secondary) should be designated by the Chief Information Security Officer (or other manager) and are be responsible for the upkeep of the firewall. The primary administrator will make changes to the firewall, and the secondary administrator will only do so in the absence of the former so that there is no simultaneous or contradictory access to the firewall. Each firewall administrator will provide a home phone number, pager number, cellular phone number, and other numbers or codes in which they can be contacted when support is required.

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 ensured. It should be required that on-call information about each firewall administrator be written down so that one may be contacted 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 has a sound understanding of network concepts and implementation. For example, since most firewalls are TCP/IP based, a thorough understanding of this protocol is compulsory. An individual that is assigned the task of firewall administration must have 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 principles and practices.

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.

**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 company firewall. Any modification of the firewall system software must be done by the firewall administrator or backup administrator and requires approval of the cognizant manager.

**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 components of a backup and recovery 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 read-only media so that data in storage is not overwritten 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 similar to the one already deployed and kept safely 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 repair. At least one firewall should be configured and reserved (not-in-use) so that in case of a firewall failure, this backup firewall can be switched on to protect the network.

**Other Firewall Policy Considerations**
Firewall technology has only been around for the last five years. In the past two years, however, firewall products have diversified considerably and now offer a variety of technical security controls that can be used in ever-more complex network connections.
This section discusses some of the firewall policy considerations in the areas of network trust relationships, virtual private networks, DNS and mail resolution, system integrity, documentation, physical firewall security, firewall incident handling, service restoration, upgrades, and audit trail logging.

**Network Trust Relationships.** Business networks frequently require connections to other business networks. Such connections can occur over leased lines, proprietary wide area networks (WANs), value added networks (VANs), or over public networks such as the Internet. For example, many local governments use leased lines or dedicated circuits to connect regional offices across the state. Many businesses use commercial VANs to connect business units across the country or the world.

The various network segments involved may be under the control of different organizations and may operate under a variety of security policies. By their very nature, when networks are connected, the security of the resulting overall network drops to the level of the weakest network. When decisions are made for connecting networks, trust relationships must be defined to avoid reducing the effective security of all networks involved.

Trusted networks are defined as networks that share the same security policy or implement security controls and procedures that provide an agreed-upon set of common security services. Untrusted networks are those that do not implement such a common set of security controls, or where the level of security is unknown or unpredictable. The most secure policy is to only allow connection to trusted networks, as defined by an appropriate level of management. However, business needs may force temporary connections with business partners or remote sites that involve the use of untrusted networks.

**Virtual Private Networks (VPNs).** Virtual private networks allow a trusted network to communicate with another trusted network over untrusted networks such as the Internet. Since some firewalls provide VPN capability, it is necessary to define policy for establishing VPNs. The following are recommended policy statements:

- Any connection between firewalls over public networks will use encrypted virtual private networks to ensure the privacy and integrity of the data passing over the public network.
- All VPN connections must be approved and managed by the network services manager.
- Appropriate means for distributing and maintaining encryption keys must be established prior to operational use of VPNs.
**DNS and Mail Resolution.** On the Internet, the domain name service (DNS) 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 an organization to maintain its own DNS database.

If the organization decides to manage its own DNS database, the firewall can (but does not 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 internal host information of a site. In other words, with the firewall acting as a DNS server, internal hosts get an unrestricted view of both internal and external DNS data. External hosts, on the other hand, do not have access to information about internal host machines. To the outside world, all connections to any host in the internal network will appear to have originated from the firewall. With the host information hidden from the outside, an attacker will not know the host names and addresses of internal hosts that offer service to the Internet. A security policy for DNS hiding might state: If the firewall is to run as a DNS server, then the firewall must be configured to hide information about the network so that internal host data is not advertised to the outside world.

**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 must be updated each time the firewall’s configuration is modified. System integrity files must be stored on read-only media or offline storage. System integrity must 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.

**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.

**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 ensure that proper environment alarms and backup systems are available so that the firewall remains online.

The firewall should be located in a 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 conditioning, and smoke alarms to ensure the proper working order of the room. The placement and recharge status of the fire extinguishers will 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.

**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 previously. The following policies are appropriate to all risk environments.

- The firewall will be configured to log all reports on daily, weekly, and monthly bases so that the network activity can be analyzed when needed.
- Firewall logs will examined on a weekly basis to determine if attacks have been detected.
- The firewall administrator will be notified at anytime of any security alarm by e-mail, pager, or other means so that he or she may immediately respond to such alarm.
- The firewall will 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 will block all software types that are known to present security threats to a network (such as ActiveX and Java) to better tighten the security of the network.

**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 are needed for restoring the firewall to a working state when a break-in occurs.

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 will 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 will be deployed.

**Upgrading the Firewall.** It is often necessary that the firewall software and hardware components be upgraded with the necessary modules to ensure 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 the following:

- To optimize the performance of the firewall, all vendor recommendations for processor and memory capacities will 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 will be obtained from a list of vendor-recommended sources. Any firewall specific upgrades will be obtained from the vendor. NFS will not be used as a means of obtaining software components. The use of virus-checked CD-ROM or FTP to a vendor's site is an appropriate method.
- The firewall administrator(s) will 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 components, the firewall administrator must verify with the vendor that an upgrade is required. After any upgrade, the firewall will be tested to verify proper operation prior to going operational.

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 change, so should security policy.
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 events 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, and inbound and outbound proxy traffic type.

CONCLUSION
Connections to external networks and to the Internet are rapidly becoming commonplace in today’s business community. These connections must be effectively secured to protect internal trusted networks from misuse and attack. The security policies outlined above should provide an effective guideline for implementing the appropriate level of controls to protect internal networks from outside attack.

Steven F. Blanding works in the Houston, TX, office of Arthur Andersen LLP.