INTERNET FIREWALLS

AN INTRODUCTION

Draft Revision 242 (26 August 1994)

Abstract

Connecting to Internet connection will expose some subset of your enterprise network resources, called the zone of risk, to Internet-based attacks from any of millions of Internet users. One way to reduce this exposure is to reduce the zone of risk to a small number of extremely secure hosts. These secure hosts are collectively referred to as a firewall. An Internet firewall allows enterprise network administrators to implement strict access controls, including strong authentication methods such as token authentication, between the Internet and the enterprise network.

Andrew T. Robinson
netMAINE
PO Box 8258
Portland, ME 04104-8258

+1 207 780.6381

atr@maine.net

TABLE OF CONTENTS

SECURITY AND THE INTERNET

An Internet connection effectively extends the enterprise network to include all 30,000+ other Internet-connected networks. This breaches the physical *security perimeter* between the enterprise network and the outside world, as illustrated in the following diagram:

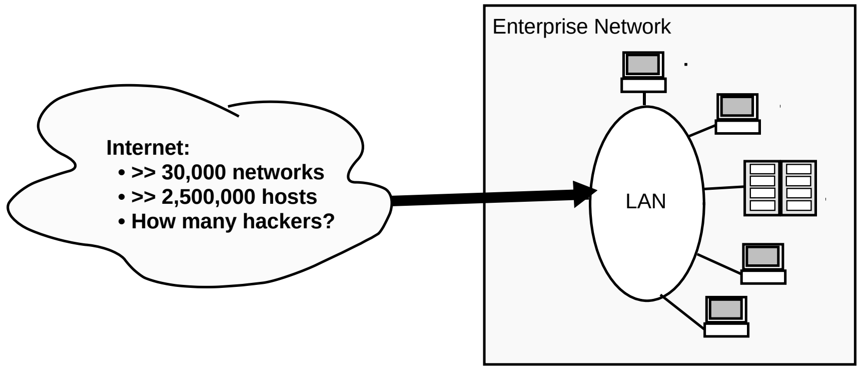

FIGURE 1: Unsecured Internet Connection

Given this method of access, it is relatively easy for a hacker to launch attacks against hosts on the enterprise network. *The goal of the hacker* may be one or all of the following:

Unauthorized access to enterprise network resources. For example, a hacker may try to login to a enterprise network host as a base to "launder" connections used to attack other enterprise network and Internet hosts.

Industrial espionage or unauthorized retrieval of the organization's secret or sensitive information. For example, a hacker may break into a enterprise network host and retrieve information about the organization's contracts, business plans, etc., to be sold to a competitor, hostile special interest group, and so on.

Sabotage. For example, a hacker could generate electronic mail which would appear to originate from an authoritative source within an organization. The contents of such forged electronic mail could cause monetary, political, or other damage to an organization.

Denial of service to legitimate users. For example, an Internet user could send one thousand (1,000) one-megabyte (1Mb) mail messages to the enterprise network mail gateway in hopes of filling the gateway's disk.

The goal of Internet security is to reestablish a strong network security perimeter which permits enterprise network users to access the Internet while preventing unauthorized Internet users from using enterprise network resources contrary to corporate security policy.

The Zone of Risk

The *zone of risk* is all TCP/IP-capable enterprise network hosts which are directly accessible from the Internet (*directly accessible* means there are no strong security measures between the Internet and the host). *Hosts within the zone of risk will be subjected to Internet-based attacks*[1] of the types described above.

Furthermore, any non-TCP/IP-capable hosts which are accessible through TCP/IP-capable enterprise network hosts (though not technically part of the zone of risk) are also vulnerable: if a hacker succeeds in gaining access to a TCP/IP-capable host, s-he can "island hop" to a non-TCP/IP-capable host to which the TCP/IP-capable host is connected.

Host Security

One way to improve security is to increase the security on all enterprise network hosts. Some of the measures which can be taken to improve the security of enterprise network hosts include:

> *Require strong passwords.* While most multi-user hosts support at least simple password protection, many users effectively bypass this security by choosing "soft" passwords which are easy to guess or crack. Host security can be measurably improved by establishing and enforcing "strong" password selection rules.
>
> *Disable unnecessary network servers.* Many network servers can be disabled on individual hosts without sacrificing any enterprise network functionality. These include electronic mail servers (a mail gateway can serve most or all of the hosts on an enterprise network), file transfer servers, etc. Any server that can be disabled is one less that a hacker can probe for weaknesses.
>
> *Provide only the privileges and access rights required to accomplish a task.* The principle of least privilege should be an axiom when managing an enterprise network connected to the Internet: assigning unnecessary privileges or access rights to a user not only increases the chance of that user abusing those privileges, but it makes it easier for a hacker to subvert the host if the hacker breaks into that user's account.

Unfortunately, since many enterprise network hosts are single-user workstations or personal computers, securing all enterprise network hosts is difficult if not possible. Legitimate users can inadvertently or purposefully subvert host-based security simply by changing the contents of a configuration file or changing a file access permission. It is desirable to increase both the level and awareness of host security, but a security administrator should not count on host security to stop Internet-based attacks.

Firewalls

The alternative is to use an Internet *firewall* to provide a "crunchy shell around the soft, chewy center" (enterprise network hosts). [Cheswick 92] A *Firewall* allows the organization to enforce its network security policy on traffic flowing between the Internet and the enterprise network. A firewall increases security by:

Reducing the zone of risk to a small number of secure systems. These systems include screening routers, encryption devices, and general-purpose hosts running security applications. Instead of worrying about security on possibly hundreds of hosts, the security administrator concentrates on firewall host security.

Establishing a strong, automated security perimeter between the Internet and the enterprise network. All traffic between the Internet and the enterprise network must pass through the firewall, where it is subject to access control, strong authentication, attack detection, and auditing.

Firewalls can be configured to implement arbitrary security policies, as illustrated below. Like security policies, firewalls range from simple and inexpensive (a screening router) to complex and expensive (screening router, bastion host(s), encryption devices, strong authentication), depending on the level of protection desired and the security policy to be implemented.

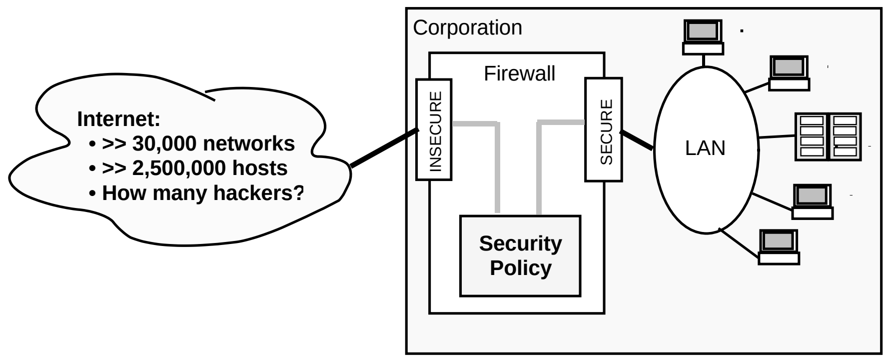

FIGURE 2: Firewall-Secured Internet Connection

FIREWALL COMPONENTS

Following are descriptions of firewall components, both hardware and software, which contribute to the cost of a firewall solution. The heading for each component description includes a range of costs for that component. Some of these ranges can be significant.

Bastion Host ($4,000-15,000+)

A bastion host is a general purpose host, usually running some version of the UNIX operating system (most firewall security applications have been designed for UNIX), which has been configured for increased security and reduced administrative complexity.

The bastion host should be configured with ample RAM and disk space. While the required configuration depends on traffic volume and usage patterns, a typical configuration would be:

Thirty-two megabytes (32Mb) RAM

One gigabyte (1Gb) hard disk

Two (2) network interface cards (NICs)

Workstations from well-known vendors such as IBM, Hewlett-Packard, DEC, and SUN, are good choices since most firewall security applications have been implemented and/or ported to these platforms. More recently, Intel-processor-based platforms running BSDI UNIX or other PC flavors of UNIX have become popular because they cost less to purchase and maintain than major vendor workstations.

Before a general purpose host can be considered a bastion host, it must be *hardened.* The hardening process reduces the host's "bug signature" and strengthens all access control, monitoring, and auditing facilities. The hardening process includes the following procedures:

All user accounts are removed except for those necessary for the operation and administration of the host (such as *maint*, *bin*, etc.)--if general users can't log in to the firewall host, they can't subvert the security measures.

All files nonessential files and executables are deleted, especially network servers (except *ftpd* and *telnetd* for administrator use) and client programs (there is no reason for anyone to *ftp* or *telnet* <u>from</u> a bastion host).

Extended logging and monitoring capabilities are configured and enabled. Preferably, log entries should be forwarded to a *log server* on the LAN. This provides an audit trail that can not be modified or deleted even if a hacker subverts the bastion host.

IP forwarding and source routing support should be disabled. This will prevent a bastion host from forwarding unauthorized packets between its two (2) network interfaces (i.e., between the Internet and enterprise network).

The TIS Firewall Toolkit ($0)

Trusted Information Systems (TIS), Incorporated, has developed a set of tools for building UNIX firewalls. This product, called the Firewall Toolkit (subsequently referred to as "the toolkit), is available at no charge from TIS over the Internet. The toolkit supports all of the firewall components described in this document.

The toolkit provides the following security applications:

An SMTP (electronic mail) gateway which permits mail transfer agent isolation and mail content screening

A "plugboard" gateway for NNTP (network news) or other protocols

FTP (file transfer) and TELNET (remote login) gateways with strong authentication interfaces

A general-purpose TCP access control facility

An authentication server which supports simple password protection, Bellcore's S/KEY, Security Dynamics' SecurID, and Digital Pathways' SNK004 Secure Net Key)

An enhanced UNIX *login* command for bastion hosts which supports the authentication server

Logging and security monitoring via an enhanced version of UNIX *syslogd*--supports triggered actions based on events which match configured regular expressions (allows real-time alerts and actions based on bastion host activity)

All of the toolkit's components share a common configuration file (/usr/local/etc/netperm-table), which simplifies administration and helps ensure continuity of access control rules. Different components of the toolkit can be mixed and matched as necessary to build a variety of firewall configurations.

Screening Router ($2,000-15,000+)

A *screening router* provides the first layer of protection for the enterprise network. A screening router can be configured to selectively permit or deny IP packets based on one or more of the following criteria.

Interface on which packet arrives (screening on input)
Source IP address
Source TCP/UDP port
Interface to which packet is routed (screening on output)
Target IP address
Target TCP/UDP port
Protocol (TCP, UDP, ICMP, etc.)
Established connections (ACK bit set in TCP header)
IP options (i.e., SOURCE-ROUTING or LOOSE-SOURCE-ROUTING)

IMPORTANT! Any screening router used in a firewall configuration should be able to screen based on any or all of these criteria. It is also important to select a router which evaluates screening rules in the order specified by the security administrator.

A properly configured screening router can close many security holes, but screening routers have the following drawbacks:

Screening routers are inflexible. The router can only permit or deny individual packets based on static rules--it does not preserve context from one packet to the next and can not make intelligent, programmed decisions about whether a particular connection or protocol operation should be allowed or denied. The screening router also can not perform logging, monitoring, or strong authentication functions beyond the functionality programmed by the vendor.

Screening rules are difficult to specify. Screening rule languages are cryptic, and some routers evaluate screening rules in an order other than that specified. This can lead to unintended consequences which can either deny legitimate access to the Internet, or permit attacks from the Internet to the enterprise network.

If the screening router is subverted, the entire network may be open to attack. Assuming the firewall consists only of a screening router, if a hacker succeeds in subverting the router s-he can reconfigure the router to allow any level of access desired.

Strong Authentication System ($0-7,500+)

Strong authentication is any authentication method which improves upon the simple password protection offered by most multi-user operating systems. Strong authentication methods include *one-time password* systems and *tokens* or *handheld authenticators* (HHAs).

One-time passwords, as the name implies, can only be used once. A different password must be used each time access is required (and different passwords may be required for different hosts). One-time passwords may be pre-generated and distributed to users in list form, or they may be generated dynamically using a challenge/response sequence.

*Tokens (*also called *Handheld authenticators* or *HHAs*) are small, self-contained computers which share a secret (such as an encryption algorithm and/or encryption key) with firewall-based authentication software. The token generates what amounts to a one-time password. The computations necessary to generate each password are performed entirely within the token. Tokens are usually further protected by a personal identification number (PIN) which is known only to the user. In order to access a host on the enterprise network, the user must have physical possession of the token *and* know the PIN.

WAN Encryption Devices ($1,500-30,000+)

WAN Encryption devices allow traffic between the enterprise network and other networks on the Internet to be automatically encrypted. Information encrypted in this way is unreadable by anyone except users on the sending and receiving networks.

The drawback of such devices is that information is encrypted only between *encryption-secured networks*, and only while the information is traversing the Internet (LAN encryption devices are also available). *Encryption-secured networks* are networks with compatible encryption devices (read this to mean networks with the same encryption device from the same vendor). Information between the enterprise network and a network with no encryption device, or an encryption device from another vendor, would *not* be protected.

WAN encryption is useful when setting up *virtual private links* (VPLs) to Internet-attached offices or business partners. For example, a corporation may want to establish an encrypted VPL with a subsidiary. This is accomplished by opening firewall "tunnels" which allow information to flow freely between the corporation and its subsidiary. An encryption device at both locations ensures that information can not be intercepted (or if it is intercepted, it is useless) and that neither network can be compromised if a hacker succeeds in "spoofing" a source IP address belonging to the other.

It is possible to set up virtual private links without using an encryption device, but such links are very vulnerable to source-address spoofing attacks and are not recommended.

Even though modern encryption algorithms are difficult to break by brute force, luck and new technology should never be discounted. There have been proposals for relatively affordable processors which can break DES keys in hours rather than years--and new technology notwithstanding, encryption keys are essentially passwords and are vulnerable if they are chosen poorly. To guard against weak encryption keys, many modern encryption platforms either dynamically and pseudo-randomly generate keys, or require strong keys. Also, platforms are available which can multiply encrypt data at very high speeds, resulting in a cipher which is (for the time being) essentially unbreakable by brute force.

SAMPLE FIREWALL CONFIGURATION

The following diagram illustrates one of many possible firewall configurations. The enterprise network is divided into a secure segment and an insecure segment (the DMZ). All traffic between the two LAN segments must pass through the bastion host. The bastion host is where most of the work of enforcing the enterprise network security policy is performed.

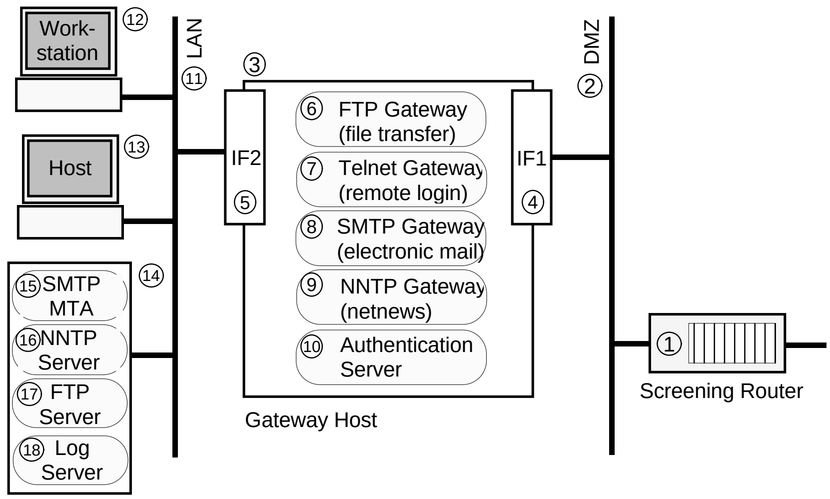

FIGURE 3: Sample Firewall Configuration

1. *Screening router:* The screening router is the first stage in the firewall, and may be used to pre-screen traffic destined for the secure LAN (11). Traffic to any DMZ-based host is permitted, including the bastion host (3). The router might also be configured to block source-routed packets and packets arriving over the Internet which claim to originate from DMZ or LAN hosts (obvious forgeries).

2. *DMZ:* This is the insecure network segment. It is insecure because the screening router permits Internet traffic to any host on the DMZ. For security purposes the DMZ can be considered part of the Internet, even though it is under the organization's administrative control.

3. *Bastion host:* The bastion host is the gateway between the LAN (11) and the DMZ (2). All traffic between the LAN and the DMZ must pass through the bastion host. The bastion host runs security applications such as those in the TIS Firewall Toolkit to facilitate the exchange of information between the Internet (DMZ) and the LAN.

   The bastion host is the only host connected to both the LAN and the DMZ (and hence to the Internet). Thus, the bastion host provides a single point of access control between the secure and insecure networks.

4. *IF1:* This is the bastion host's network interface (NIC) to the DMZ (2). It is assigned an address within the IP subnet address space used for the DMZ.

5. *IF2:* This is the bastion host's network interface (NIC) to the LAN (11). It is assigned an address within the IP subset address space used for the LAN.

6. *FTP gateway:* The FTP gateway controls FTP access between the LAN (11) and the DMZ/Internet (2). A LAN user can use the FTP gateway to access any Internet-based host. An Internet user attempting public anonymous FTP would automatically be routed to the FTP server on the Internet Service Host (14). An Internet user attempted to FTP to any other LAN host would be required to strongly authenticate the access via the authentication server (10).

7. *Telnet gateway:* The Telnet gateway controls Telnet access between the LAN (11) and the DMZ/Internet (2). A LAN user can use the Telnet gateway to access any Internet-based host. An Internet user attempting to Telnet to a LAN host (13) or workstation (12) would be required to strongly authenticate the access via the authentication server (10).

8. *SMTP gateway:* The SMTP gateway (8) prevents Internet users from communicating interactively with the potentially buggy SMTP mail transfer agent (15). The gateway simple accepts SMTP connections, writes incoming mail to disk, and notifies the MTA of the mail.

9. *NNTP gateway:* The NNTP gateway is similar to the SMTP gateway: it acts as a middleman between an NNTP netnews server on the LAN (16) and an Internet-based NNTP newsfeed.

10. *Authorization server:* The authorization server may be used by any of the application gateways (6-9) to verify the identity of a connection request using strong authentication techniques such as one-time passwords or handheld authenticators (HHAs, tokens).

11. *LAN:* This is the secure local area network (LAN). This LAN is secure in the sense that there is no direct connection between the LAN and the DMZ/Internet (2)--all traffic between the LAN and the DMZ/Internet must flow through the bastion host (3).

12. *Workstation:* This is a single-user workstation on the secure LAN (11). This workstation may run UNIX or any personal computer operating system. The security level of such workstations may vary widely depending on the operating system and configuration.

13. *Host:* This is a multi-user host on the secure LAN (11). The host may be anything up to a large mainframe system. Most modern timesharing hosts have the capability of at least C2 security [DOD 85].

14. *Internet service host:* In this example, the Internet Service Host is a dedicated machine which runs certain network applications. The Internet Service Host is configured as a firewall host, and as such does nothing other than support the designated network functions (in this case, SMTP, NNTP, and FTP). It is possible to distribute these functions across several hosts, and it is not strictly necessary that these hosts be configured as firewall hosts if confidence in the security of the bastion host is high.

15. *SMTP MTA:* This is the SMTP electronic mail transfer agent. A common SMTP, *sendmail*, has traditionally presented a significant security exposure. Because of this, the MTA is isolated on the LAN and DMZ/Internet users can not access it interactively--all mail is relayed from the SMTP gateway to the MTA. This does not totally eliminate the danger of mail content attacks (for example, using piping and redirection symbols in mailing addresses), but the SMTP gateway may pre-screen incoming mail for known content attacks.

16. *NNTP server:* This is a netnews server. NNTP traffic is relayed to and from an Internet-based NNTP newsfeed.

17. *FTP server:* This is the public anonymous FTP server. Information to be made available to the public can be made available through this server. The FTP server should run in an isolated directory (users must not be able to gain arbitrary access to the directory structure) and this directory should be maintained to eliminate obsolete and unnecessary files on a regular basis.

18. *Log server:* This server accepts auditing and security event messages from the bastion host, screening router, and other hosts and processes participating in the firewall. Having the logging server on the secure LAN (11) adds another level of protection to the firewall: even if a hacker breaks into the firewall, s-he can not destroy the audit trail without also breaking into the Internet service host.

This firewall implementation has the following important characteristics:

Reduced zone of risk. The zone of risk in this example includes only the screening router (1) and the bastion host (3), thus restoring the security perimeter of the LAN (11).

Defense-in-depth. This configuration provides an interlocking set of defenses which provide attack prevention, detection, and tracking capabilities. The screening router (1) blocks many types of attacks using screening rules. This is backed up by the bastion host (3) which is the primary agent for enforcing the organization's security policy for Internet traffic. If the bastion host is compromised, it can not be used by the attacker to launch attacks against secure LAN (11) hosts. Even if the attacker reconfigures bastion host access control, only the Internet service host (14)--also a secure host--has any special trust relationship with the bastion host. Attack detection and tracking capabilities of the bastion host (3) allow the attack to be detected and remedial measures (such as shutting down the Internet connection and notifying security administrators) can be performed automatically.

Centralized security administration. The Internet security administrator needs to maintain only three (3) hosts: the screening router (1), the bastion host (3), and the Internet service host (14). After initial configuration, only the bastion host (3) will need consistent attention.

Although this is a fairly strong configuration, it is not perfect. Some improvements would include moving the log server (18) to its own host (as configured above, a user who compromised the Internet service host (14) would be able to destroy the audit trail), and to add another bastion host and another intermediate network between the current bastion host (3) and the secure LAN (12). This second bastion host could monitor the first and report any changes in configuration or behavior, and would create yet another level of security which the hacker would have to penetrate to access the secure LAN. Unfortunately, stronger configurations become progressively more expensive.

IMPLEMENTATION COST ESTIMATES

Following are estimates for this sample configuration and several options. *These are rough estimates,* based on costs provided in the ***FIREWALL COMPONENTS*** section. Some costs may be eliminated as follows:

> *All estimates include the cost of a new bastion host.* If a suitably configured machine is already available, the estimates may be reduced by at least $5,000.
>
> *Several estimates include the cost of a new Internet service host.* If suitably configured machines are available to assume these functions, the estimates may be reduced by at least $5,000.
>
> *Several estimates include the cost of a screening router.* If a suitably configured screening router is already available, the estimates may be reduced by at least $2,250.
>
> *All estimates include an estimated consulting fee to implement the firewall configuration.* If the organization has suitable expertise and/or confidence in-house, the estimates may be reduced by at least $7,500.

Sample Firewall Configuration ($24,500)

(1) Bastion host hardware (BSDI Unix, 486/66, 32Mb RAM, 1Gb DASD)	$ 7,000
(1) Internet service host hardware (OS/2, 486/66, 16Mb RAM, 1Gb DASD)	$ 5,000
(1) Screening router (Network Systems 6601)	$ 5,000
(1) Firewall software (TIS Firewall Toolkit)	-n/c-
(1) Authentication server (Bellcore S/KEY)	-n/c-
Implementation by security consultant (not including security policy planning)	$ 7,500
TOTAL	**$24,500**

Option 1: SecureNet Key Authentication System ($27,500)

(1) Bastion host hardware (BSDI Unix, 486/66, 32Mb RAM, 1Gb DASD)	$7,000
(1) Internet service host hardware (OS/2, 486/66, 16Mb RAM, 1Gb DASD)	$5,000
(1) Screening router (Network Systems 6601)	$5,000
(50) Authentication tokens (SNK004 @ $60 per token)	$3,000
(1) Firewall software (TIS Firewall Toolkit)	-n/c-
Implementation by security consultant (not including security policy planning)	$7,500
TOTAL	**$27,500**

Option 2: SecurID Authentication System ($35,000)

The SecurID server software, ACE/Server, has not been released for Intel-based UNIX platforms--this option specifies a SunOS system instead. Other options include DEC ULTRIX and IBM AIX systems.

(1) Bastion host hardware
  (SunOS, Sun, 32Mb RAM, 1Gb DASD) $10,000
(1) Internet service host hardware
  (OS/2, 486/66, 16Mb RAM, 1Gb DASD) .... $ 5,000
(1) Screening router (Network Systems 6601) .... $ 5,000
(1) Authentication server
  (SecurID ACE/Server, 50 user)) .... $ 5,000
(50) Authentication tokens
  (SecurID @ $50 per token) .... $ 2,500
(1) Firewall software
  (TIS Firewall Toolkit) .... -n/c-

Implementation by security consultant
  (not including security policy planning) .... $ 7,500

TOTAL $35,000

Option 3: Combined Gateway and Internet Service Hosts ($22,500)

(1) Gateway and Internet service host hardware
  (BSDI UNIX, 486/66, 64Mb RAM, 2 x 1Gb DASD) $10,000
(1) IP router (Network Systems 6601) .... $ 5,000
(1) Authentication server
  (Bellcore S/KEY one-time-password system) .... -n/c-
(1) Firewall software
  (TIS Firewall Toolkit) .... -n/c-

Implementation by security consultant
  (not including security policy planning) .... $ 7,500

TOTAL...$22,500

Option 4: Smaller Organizations ($14,750)

(1) Gateway and Internet service host hardware
  (BSDI UNIX, 486/50, 16Mb RAM, 1 x 1Gb DASD) .... $ 5,000
(1) Screening router (Morning Star EXPRESS) .... $ 2,250
(1) Authentication server
  (Bellcore S/KEY one-time-password system) .... -n/c-
(1) Firewall software
  (TIS Firewall Toolkit) .... -n/c-

Planning, installation, and configuration labor .... $ 7,500

TOTAL $14,750

ENDNOTES

[1] Innocent or well-meaning *probes* of the enterprise network and network services may be far more common than actual attacks. For example, a user who tries to use the *FINGER* function to find out an employee's name probably means no harm. Unfortunately, probes are frequently used as precursors to attacks--and using the previous example, the *FINGER* function can provide information and even a back door to a knowledgeable hacker.

BIBLIOGRAPHY

[Bellovin 92] Bellovin, Steven M., *There Be Dragons*, August 1992

[Bellovin 93] Bellovin, Steven M., *Packets Found on the Internet*, July 1993

[BelMer 91] Bellovin, Steven M., Merritt, Michael, *Limitations of the Kerberos Authentication System*, Winter 1991

[Chapman 92] Chapman, Brent D., *Network (In)security Through IP Packet Filtering*, September 1992

[ChesBel 94] Cheswick, William R., Bellovin, Steven M., *Firewalls and Internet Security*, April 1994

[Cheswick 90] Cheswick, W. R., *The Design of a Secure Internet Gateway*, June 1990

[Cheswick 92] Cheswick, W. R., *An Evening with Berferd*, January 1992

[HalKarn 92] Haller, Neil M., Karn, Phillip R., *Description of the S/KEY One-Time Password System*, 1992

[HolRey 91] Holbrook, P., Reynolds, J., *RFC 1244: Site Security Handbook*, July 1991

[Ranum 92] Ranum, Marcus J., *A Network Firewall*, June 1992

[Ranum 93] Ranum, Marcus, J., *Thinking About Firewalls*, 1993

[Steiner 88] Steiner, Jennifer G. et al, *Kerberos: An Authentication Service for Open Network Systems*, March 1988

[Wallich 94] Wallich, Paul, "Wire Pirates", *Scientific American*, March 1994