How To Build And Run A Firewall

We take a look at some of the issues involved in choosing, setting-up and running a firewall.

By Simon Bisson

Now that corporate access to the Internet is seen as a business advantage, more and more companies are finding themselves having to think long and hard about the security implications of a connection.

With attacks on business computer systems becoming more visible (and potentially more expensive), and with holes in operating systems more public, some form of Internet security policy is essential. This can include everything from limiting the number of machines and systems with an Internet connection, to controlling what files can enter or leave a company network. A security policy alone won't prevent attacks and intrusions, so some form of defence is required, often implemented in the form of a firewall.

Definition

A firewall is a set of tools designed to prevent unauthorised access to a network, and can mix hardware and software solutions to provide a layered defence. A typical firewall architecture is based around two concepts: the "choke router" and the "bastion host" [*refer also to Understanding Firewalls, File S0499, PCNA Issue 86 - Ed.*].

Most routers allow you to define access control lists, which can control exactly which IP packets are routed and to where. Whilst choking an Internet connection this way is an all-or-nothing security mechanism, you can use router access control lists to explicitly deny access to your network for specific packet types, or to make sure that certain packets are only delivered to specific machines so that, for example, mail is only delivered to your mail server or Web access is only to your public Web server or Web proxies.

Bastion Host

Keeping the network itself secure is the job of the bastion host. Taking its name from the fortified gateways of a feudal Norman castle, this is what is often thought of as the firewall but is really only part of a layered firewall architecture.

The bastion host is a machine with only one purpose: to pass packets between your network and the Internet. Usually, it's a dedicated machine with two separate network interfaces. The bastion host will act as an active router, linking your private network to the Internet, monitoring the state of connection and blocking packets that don't meet the rules you have defined.

If you use it for anything else than as an Internet gateway, you may be adding weaknesses to a security architecture. For example, if you use the machine for reading email, it's possible for someone to send an email with an embedded ActiveX control so that, when you read the message, the control turns off the firewall.

You must make sure that the bastion's operating system is configured to prevent any packets being routed directly between its network interfaces. Most commercial packages will handle this for you, but if you are unsure, you can configure most dialects of Unix to stop any internal routing.

The DMZ

Between the choke router and the bastion host lies the "Demilitarised Zone". The DMZ is a partially protected area, where you can install public services. Machines in the DMZ should not be fully trusted, and should only be used for single purposes - such as a Web server or an ftp server. Any extra services should be disabled, and user accounts kept to a minimum. If it is possible to only allow logins from trusted hosts or the system console, all other access routes should be removed.

Some firewall packages make the DMZ more secure by using a third network interface to host public services and using the firewall software to protect them rather than a choke router.

Firewall Policies

It's sometimes best to think of Internet security policies in terms of the "Four Ps", namely Paranoia, Pragmatism, Permissiveness and Promiscuity. Each approach is the result of a different assessment of the risks involved in opening a corporate network to the Internet:

- A Paranoid network is never connected to the Internet.
- A Pragmatic network only permits selected applications and services access to the Internet, and blocks all others.
- A Permissive network lets all applications have access to the Internet, except for those specifically seen as a threat.
- A Promiscuous network is connected directly to the Internet, and lets all applications and services have full access to and from the Internet.

One of the best techniques for securing a network is to hide it from the Internet. A range of IP addresses is reserved for intranet use, and allows you to build as large a network as you like, as long as you use some form of network address translation to allow packets to travel into and out of your network.

Documented in RFC 1918 "Address Allocation for Private Internets", the reserved addresses are allocated in three ranges: a single Class A address from 10.0.0.0 to 10.255.255.255; 16 Class B addresses from 172.16.0.0 to 172.31.255.255; and 255 Class C addresses from 192.168.0.0 to 192.168.255.255.

The available address space is larger than most companies will ever need, and allows you to develop your own network numbering scheme quickly. Moving an existing network to one of these address schemes is a tricky process, but if handled correctly can be achieved with little or no disturbance. Using these reserved addresses, and an address-translating firewall, you can keep your internal systems from direct external access, providing pathways through the firewall only to trusted hosts or to specific services. Network address translation is a standard feature with most modern application gateway-based firewalls, or can be added as an optional extra to packet filter-based systems.

Choosing A Firewall

Two basic technologies are used to build active firewalls, namely stateful packet filters and application gateways. These operate in different ways, and have different effects on how you run your Internet connection.

It is relatively simple to block access using packet filtering techniques, which can allow or prevent access to services from specific machines. This can be carried out either at a high level on a site's access routers or specifically on a firewall machine. A router alone cannot fully control a stream of IP packets, as it cannot monitor the state of incoming and outgoing packets - so some protocols like ftp which use more than one datastream present problems for a router-based firewall.

Things get worse when you use a connectionless protocol like UDP, which forms the basis of essential Internet services like DNS. In order to control UDP streams in a firewall, you need to add some form of state monitoring to a packet filter, so that the firewall can control access based on packet requests and sophisticated rules (see Figure 1).

At a higher level, application- and circuit-level gateways act as routers that pass only specific packets on to specific machines (eg, HTTP requests to a Web server, or SMTP packets to a mail server). You can use application gateways to transmit only application-specific data across a firewall, which can be processor-intensive. Circuit-level gateways open a virtual circuit on receiving a valid handshake, but do not analyse packet traffic, and in some cases require use of modified software - especially true in the case of the commonly used SOCKS gateway package. These gateway techniques have a considerable advantage over packet filtering techniques in that the true network address of a protected machine is always hidden from any external networks (see Figure 2).

There are a large number of firewall tools available, for virtually every operating system. It's worth looking at the various Internet resources available before choosing a firewall, and then trying one or two evaluation copies before you decide what to use. You'll find there are tools that suit every budget, from the free TIS Firewall Toolkit, through to the cheap and powerful GNATbox, to the heavy-hitting corporate firewalls from Digital with AltaVista Firewall 97 and Checkpoint's Firewall-1, as well as Raptor's Eagle and TIS's (now part of Network Associates) Gauntlet.

Next Steps

Once you've built a firewall, you can add extra features. One useful addition is the use of a virus checker like MIMEsweeper between an email gateway and your SMTP mailer, so all encapsulated files are virus-checked before entry into a system.

Not Firewalls

Remember that a gateway tool or a proxy server is not a firewall. Packages like Wingate or the Microsoft Proxy Server make it easy for you to connect a small network to the Internet. However, they don't protect it from intrusion or from malicious use of your resources. There have been an increasing number of cases where spammers have used proxied mail servers to relay unsolicited commercial email, at considerable cost to the owners of the systems that were hijacked.

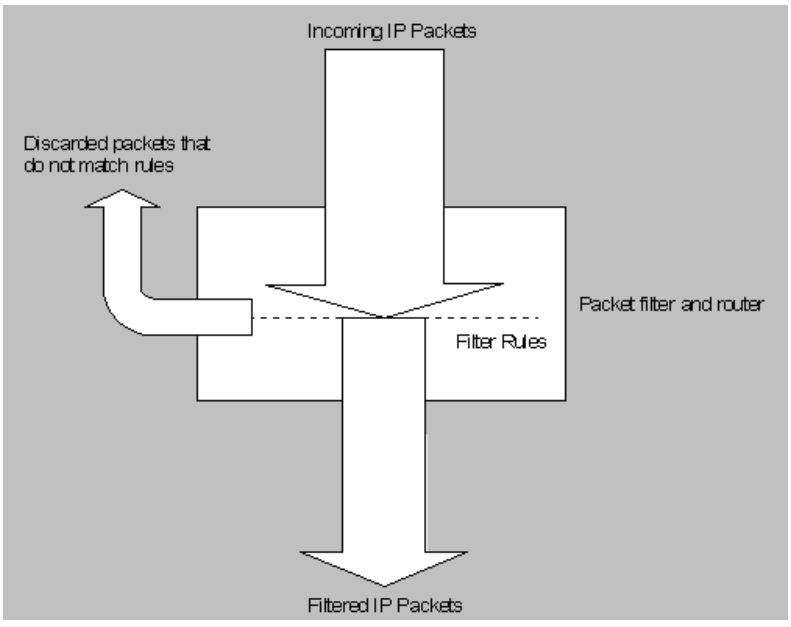

Figure 1 - State Monitoring.

Firewalls

Running A Firewall

Once you've chosen a firewall, you can begin to define the rules and procedures you will use to defend your systems. As an example, I'll look in more detail at Digital's AltaVista Firewall 97 package. One of the more common firewalls, it is available both for most major Unix dialects and Windows NT. AltaVista Firewall 97 is based around the linked concepts of trusted hosts, and application- and circuit-level gateways. Using these, you can control access to the Internet from your internal systems, and also to your internal systems from the Internet.

A trusted host is a machine that you have allowed access to your resources from the Internet, and is owned and operated either by your organisation or a partner company. You can allow these systems limited access through the firewall, usually on a specific services basis. An application gateway acts as a secure proxy, and limits access to Internet services, either by authorising users or by trusted hosts. Application gateways will also monitor the behaviour of a connection, and flag warnings if specific alarm thresholds are crossed.

Once you've installed it, AltaVista Firewall will start up in a "paranoid" mode, with all access through the firewall disabled, apart from the basic Web and mail proxies. All other proxies must be configured before being started, allowing you to build a pragmatic security policy.

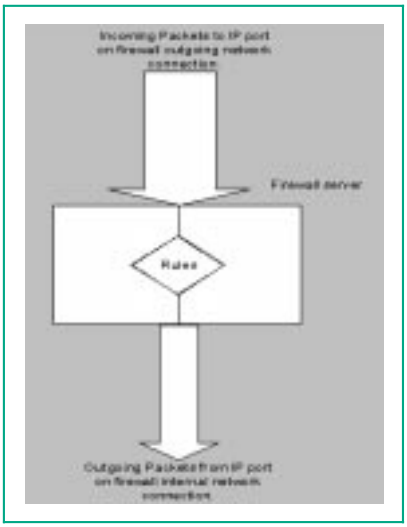

Figure 2

Application Gateways

AltaVista Firewall is designed to control access to services on internal and external networks. This is achieved by using trusted proxies for all services that require a connection. In this environment, users and systems on your internal network do not connect directly to the Internet, and direct external access is prevented, with all internal and external connections carried through the firewall's trusted proxies.

The AltaVista trusted proxies carry out the following security checks:

- The proxy checks the IP number of the requesting system. If it is not authorised, connections will be rejected.
- Some proxies limit the available operations to a subset of the full service.
- All connections and attempted connections are logged.

You'll find that AltaVista installs the following proxies:

- HTTP - for Web connections.
- ftp - for file transfers.
- Telnet - for remote terminal access.
- SMTP - for Internet email.
- NNTP - for access to news servers.
- RealAudio - for cross-Internet multimedia.
- Generic - for custom applications.
- SQL*Net - for access to Oracle databases.
- Finger - to see if someone is online.

You probably will only require a limited number of these proxies. Initially internal desktop systems should only be allowed access to World Wide Web connections, with specific systems being given ftp access if required.

Event Logs

You can use AltaVista Firewall to log all significant events. These include network connections, mail transactions and all uses of proxies. You can use the logs to produce reports and to generate alerts for your system administration team. Log files are created daily, and are stored in date-specific directories. They are not deleted automatically, and will need to be deleted manually.

Alarms

The AltaVista Firewall continually monitors firewall activity. When a potentially dangerous event is detected, the alarm system is used to determine the action to be taken. Each service has a default alarm configuration. You can fine-tune these from the firewall GUI. Alarms are built around user-defined rules, and are used to trigger various responses, up to and including closing down all firewall activity (thus not allowing any traffic through).

Reports

AltaVista Firewall uses the system logs to generate various reports on system activity and security. By default, a summary report is mailed to the system administrator, but you can customise report types, and their destination and frequency. Reports can be automatically mailed daily, weekly or monthly, and are generated just after midnight. Individual reports can indicate:

- The 10 largest transfers.
- The 10 longest transfers.
- The 10 most frequent users.
- The 10 days with most frequent connections.

Application Gateways

The AltaVista Firewall WWW proxy acts as a gateway from internal systems to the Internet at large. The proxy accepts connections from internal systems, rewrites the network address, and requests data from the target external Web servers. You can configure the WWW proxy to allow access from specific IP addresses, and so control access by your users, by adding and removing IP addresses to and from a list.

You can also use the WWW proxy as a Web cache to improve Web access for users. A heavily-used cache can take up a lot of disk space, so initially

the Web proxy should be configured without a cache. If log analysis shows that certain sites are accessed regularly, you can then setup a cache. It's a good idea to set the cache lifetime to a week, and sites with a high number of dynamic pages should be excluded from the cache.

If casual Internet use is a problem, AltaVista Firewall can be used to block access to specific sites. This list is then applied globally to all outgoing HTTP proxy connections. In order to prevent access to a banned site the site name or IP address will need to be specified, with wild cards to prevent access to specific directories. As AltaVista only has explicit blocks, to ensure that sites are completely blocked they should be listed by both name and IP number, otherwise your users could find a way around your blocks.

If you want to use ftp, you'll find that by default the AltaVista firewall proxy prevents access from external systems to internal resources. You can apply time restrictions to the proxy, so you can limit access to normal working hours. Unless a user is required to use ftp as part of his or her everyday tasks it is recommended that details of how to connect to the ftp proxy only be given when required, and that the firewall ftp logs are monitored for unauthorised usage.

If you're using Windows NT, access to ftp can be limited to users who have authenticated NT user IDs. This will require that the server is part of an NT domain, and that you've set up AltaVista Firewall to use NT user authentication. You can also use a blacklist to prevent specific machines from accessing ftp resources. The blacklist is a list of DNS names and IP numbers, and is common to the ftp, telnet, generic, news, RealAudio, SQL*Net and finger proxies, but can be applied to these proxies only when required.

The firewall can be used as a standard SMTP mail relay, passing mail between internal and external systems. It will check all incoming mail to ensure that it is sent from a valid host, it is not being sent to a file or a program and it contains no forbidden SMTP keywords. Outgoing mail is processed to ensure that it is a valid SMTP message, received headers are removed for hidden DNS environments, and "From:" headers are rewritten to ensure compliance with any corporate standards.

Generic Proxy

If you're using Internet applications that AltaVista Firewall doesn't have a built in proxy for, you can use the generic proxy to create custom proxies for these services. AltaVista Firewall's generic TCP proxy uses the TCP/IP protocol's port and socket model to allow connections for a specific port to be relayed from one side of the firewall to another. You can create multiple proxies, with unique names and port numbers. A generic proxy can be associated with specific source and destination addresses, allowing application tunnels to be created. This can be used to prevent unauthorised access to specific applications and services, by limiting access to specific hosts or subnets.

Testing A Firewall

Once you've built and installed a firewall, it's never safe to assume that your network is completely secure. Recent figures indicate that a substantial percentage of intrusions are into sites that have firewalls. You should regularly test your firewall with the latest security scanning tools, as well as keeping up to date with the security community's latest bulletins by subscribing to the BUGTRAQ and Firewalls mailing lists.

One of the best tools, and most notorious, is Dan Farmer's SATAN. One of the most respected Internet security professionals, Farmer worked with long-time collaborator (and author of the powerful TCP Wrapper firewall tool) Wietse Venema to produce a program to automate various techniques that probe a network's defences, and to produce a report of its weaknesses.

Freely available over the Internet, SATAN is easy to use, and can be used to create a database of vulnerabilities for every machine on your public Internet-facing network - including your firewall. As SATAN can be used by both network administrators and crackers, it's sensible to scan your system with SATAN and patch any vulnerabilities as soon as you set up any Internet connection. Whilst SATAN is easy to use, you'll need a Unix machine and some Perl skills to get it working.

If you'd prefer to use a commercial package, then ISS's SAFEsuite is designed to scan a wide range of different systems, and will run on most major dialects of Unix and Windows NT. A key component of SAFESuite is the System Security Scanner, which will run on both internal and external systems, and highlight any security vulnerabilities, including verifying that the latest operating system patches have been added. You can also use tools like this to make sure that no Trojan Horse backdoors have been installed on your system by attackers.

There's also a dedicated firewall test utility, which will highlight everything from minor configuration errors to potential back doors to cases where someone has simply forgotten to switch the firewall on. Details can be found at http://www.iss.net.

Conclusion

A firewall alone is no substitute for a good security policy. To keep a company safe and secure, the hardware and software must be backed up with policies and procedures designed to keep watch on the latest operating system bugs and intrusions, and the latest tools and techniques used by crackers. Of course, never forget that most attacks on computer systems are carried out from inside an organisation, by its employees.

PCNA

The Author

Simon Bisson is an Internet system architect and was previously technical manager for an Internet service provider.

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.