# Firewalls and Internet Security - The Internet Protocol Journal - Volume 2, No. 2



**Firewalls and Internet Security, the Second Hundred (Internet) Years**
by Frederic Avolio, Avolio Consulting

Interest and knowledge about computer and network security is growing along with the need for it. This interest is, no doubt, due to the continued expansion of the Internet and the increase in the number of businesses that are migrating their sales and information channels to the Internet. The growth in the use of networked computers in business, especially for e-mail, has also fueled this interest. Many people are also presented with the postmortems of security breaches in high-profile companies in the nightly news and are given the impression that some bastion of defense had failed to prevent some intrusion. One result of these influences is that that many people feel that Internet security and Internet firewalls are synonymous. Although we should know that no single mechanism or method will provide for the entire computer and network security needs of an enterprise, many still put all their network security eggs in one firewall basket.

Computer networks may be vulnerable to many threats along many avenues of attack, including:

- Social engineering, wherein someone tries to gain access through social means (pretending to be a legitimate system user or administrator, tricking people into revealing secrets, etc.)
- War dialing, wherein someone uses computer software and a modem to search for desktop computers equipped with modems that answer, providing a potential path into a corporate network
- Denial-of-service attacks, including all types of attacks intended to overwhelm a computer or a network in such a way that legitimate users of the computer or network cannot use it
- Protocol-based attacks, which take advantage of known (or unknown) weaknesses in network services
- Host attacks, which attack vulnerabilities in particular computer operating systems or in how the system is set up and administered
- Password guessing
- Eavesdropping of all sorts, including stealing e-mail messages, files, passwords, and other information over a network connection by listening in on the connection.

Internet firewalls have been around for a hundred years-in Internet time. Firewalls can help protect against some of these attacks, but certainly not all. Firewalls can be very effective at what they do. The people who set up and use them must have the knowledge of how they work, and also be aware of what they can and cannot protect. In this article, we examine the Internet firewall, touch on its history, see how firewalls are used today, and discuss changes that are in place for the next hundred years.

Internet History

In the beginning, there was no Internet. There were no networks. There was no e-mail, and people relied on postal mail or the telephone to communicate. The very busy sent telegrams. Few people used ugly names to refer to others whom they had never met. Of course, the Internet has changed all this. The Internet, which started as the Advanced Research Projects Agency Network (ARPANET), was a small, almost closed, community. It was a place, to borrow a line from the theme to Cheers, "where everybody knows your name, and they're always glad you came."

On November 2, 1988, something happened that changed the Internet forever. Reporting this incident, Peter Yee at the NASA Ames Research Center sent a note out to the TCP/IP Internet mailing list that reported, "We are currently under attack from an Internet VIRUS! It has hit Berkeley, UC San Diego, Lawrence Livermore, Stanford, and NASA Ames." Of course, this report was the first documentation of what was to be later called The Morris Worm. The researchers and contributors that had built the Internet, as well as the organizations that were starting to use it, realized at that moment that the Internet was no longer a closed community of trusted colleagues. In fact, it hadn't been for years. To their credit, the Internet community did not overreact to this situation. Rather, they started sharing information on their practices to prevent future disruptions.

(One of the results of this problem was a growth in the number of Internet mailing lists dedicated to security and bug tracking. The firewalls list-subscribe with e-mail to Majordomo@lists.gnac.net -and the bugtraqs list-LISTSERV@netspace.org -are two examples, as well as the CERT Coordination Center-http://www.cert.org/ .) Other famous, and general, attacks followed:

- Bill Cheswick's "evening with Berferd" [4]
- Clifford Stoll's run-in with German spies [7]
- The massive password capture of the winter of 1994
- The IP spoofing attack that Kevin Mitnick used against Tsutomu Shimomura [6]
- The rash of denial-of-service attacks in January 1996, and the "Web site break-in of the week."

All these viruses have made it into the popular press, and all have raised awareness of the need for good computer and network security. As these, and other, events were unfolding, the firewall was starting its rapid evolution. Although the development of firewall technology and products may be seen as very fast, it sometimes seems that firewalls are just barely keeping up with the new applications and services that spring up and immediately become a "requirement" for many Internet users.

Firewall History

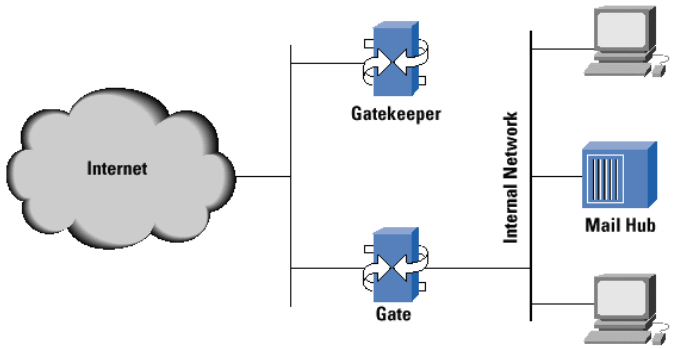
We are used to firewalls in other disciplines, and, in fact, the term did not originate with the Internet. We have firewalls in housing, separating, for example, a garage from a house, or one apartment from another. Firewalls are barriers to fire, meant to slow down its spread until the fire department can put it out. The same is true for firewalls in automobiles, segregating the passenger and engine compartments. Cheswick and Bellovin, in the definitive text on Internet firewalls [4] , said an Internet firewall has the following properties: it is a single point between two or more networks where all traffic must pass (choke point); traffic can be controlled by and may be authenticated through the device, and all traffic is logged. In a talk, Bellovin later stated, "Firewalls are barriers between 'us' and 'them' for arbitrary values of 'them.'" The first network firewalls appeared in the late 1980s and were routers used to separate a network into smaller LANs. In these scenarios and using Bellovin's definition, above "us" might be well, "us." And "them" might be the English Department. Firewalls like this were put in place to limit problems from one LAN spilling over and affecting the whole network. All this was done so that the English Department could add any applications to its own network, and manage its network in any way that the department wanted. The department was put behind a router so that problems due to errors in network management, or noisy applications, did not spill over to trouble the whole campus network. The first security firewalls were used in the early 1990s. They were IP routers with filtering rules. The first security policy was something like the following: allow anyone "in here" to access "out there." Also, keep anyone (or anything I don't like) "out there" from getting "in here." These firewalls were effective, but limited. It was often very difficult to get the filtering rules right, for example. In some cases, it was difficult to identify all the parts of an application that needed to be restricted. In other cases, people would move around and the rules would have to be changed.

The next security firewalls were more elaborate and more tunable. There were firewalls built on so called bastion hosts. Probably the first commercial firewall of this type, using filters and application gateways (proxies), was from Digital Equipment Corporation, and was based on the DEC corporate firewall. Brian Reid and the engineering team at DEC's Network Systems Lab in Palo Alto originally invented the DEC firewall. The first commercial firewall was configured for and delivered to the first customer, a large East Coast-based chemical company, on June 13, 1991. During the next few months, Marcus Ranum at Digital invented security proxies and rewrote much of the rest of the firewall code. The firewall product

was produced and dubbed DEC SEAL (for Secure External Access Link). The DEC SEAL was made up of an external system, called Gatekeeper, the only system the Internet could talk to, a filtering gateway, called Gate, and an internal Mailhub (see Figure 1).

In this same time frame, Cheswick and Bellovin at Bell Labs were experimenting with circuit relay-based firewalls. Raptor Eagle came out about six months after DEC SEAL was first delivered, followed by the ANS InterLock.

Figure 1: DEC SEAL-First Commercial Firewall




*Note:Click above for larger view

On October 1, 1993, the Trusted Information Systems (TIS) Firewall Toolkit (FWTK) was released in source code form to the Internet community. It provided the basis for TIS' commercial firewall product, later named Gauntlet. At this writing, the FWTK is still in use by experimenters, as well as government and industry, as a basis for their Internet security. In 1994, Check Point followed with the Firewall-1 product, introducing "user friendliness" to the world of Internet security. The firewalls before Firewall-1 required editing of ASCII files with ASCII editors. Check Point introduced icons, colors, and a mouse-driven, X11 based configuration and management interface, greatly simplifying fire-wall installation and administration.

Early firewall requirements were easy to support because they were limited to the Internet services available at that time. The typical organization or business connecting to the Internet needed secure access to remote terminal services (Telnet), file transfer (File Transfer Protocol [FTP]), electronic mail (Simple Mail Transfer Protocol [SMTP]), and USENET News (the Network News Transfer Protocol-NNTP). Today, we add to this list of "requirements" access to the World Wide Web, live news broadcasts, weather information, stock quotes, music on demand, audio and videoconferencing, telephony, database access, file sharing, and the list goes on.

What new vulnerabilities are there in these new "required" services that are daily added to some sites? What are the risks? Too often, the answer is "we don't know."

Types of Firewalls

There are four types of Internet firewalls, or, to be more accurate, three types plus a hybrid. The details of these different types are not discussed here because they are very well covered in the literature. [1, 3, 4, 5]

Packet Filtering

One kind of firewall is a packet filtering firewall. Filtering firewalls screen packets based on addresses and packet options. They operate at the IP packet level and make security decisions (really, "to forward, or not to forward this packet, that is the question") based on the headers of the packets.

The filtering firewall has three subtypes:

- Static Filtering, the kind of filtering most routers implement-filter rules that must be manually

changed

- Dynamic Filtering, in which an outside process changes the filtering rules dynamically, based on router-observed events (for example, one might allow FTP packets in from the outside, if someone on the inside requested an FTP session)
- Stateful Inspection, a technology that is similar to dynamic filtering, with the addition of more granular examination of data contained in the IP packet

Dynamic and stateful filtering firewalls keep a dynamic state table to make changes to the filtering rules based on events.

Circuit Gateways

Circuit gateways operate at the network transport layer. Again, connections are authorized based on addresses. Like filtering gateways, they (usually) cannot look at data traffic flowing between one network and another, but they do prevent direct connections between one network and another.

Application Gateways

Application gateways or proxy-based firewalls operate at the application level and can examine information at the application data level. (We can think of this as the contents of the packets, though strictly speaking proxies do not operate with packets.) They can make their decisions based on application data, such as commands passed to FTP, or a URL passed to HTTP. It has been said that application gateways "break the client/server model."

Hybrid firewalls, as the name implies, use elements of more than one type of firewall. Hybrid firewalls are not new. The first commercial firewall, DEC SEAL, was a hybrid, using proxies on a bastion host (a fortified machine, labeled "Gatekeeper" in Figure 1), and packet filtering on the gateway machine ("Gate"). Hybrid systems are often created to quickly add new services to an existing firewall. One might add a circuit gateway or packet filtering to an application gateway firewall, because it requires new proxy code to be written for each new service provided. Or one might add strong user authentication to a stateful packet filter by adding proxies for the service or services.

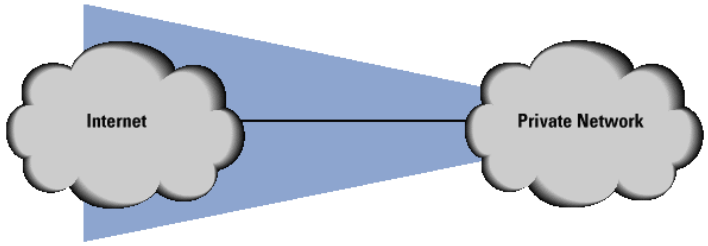
No matter what the base technology, a firewall still basically acts as a controlled gateway between two or more networks through which all traffic must pass. A firewall enforces a security policy and it keeps an audit trail.

What a Firewall Can Do

A firewall intercepts and controls traffic between networks with differing levels of trust. It is part of the network perimeter defense of an organization and should enforce a network security policy. By Cheswick's and Bellovin's definition, it provides an audit trail. A firewall is a good place to support strong user authentication as well as private or confidential communications between firewalls. As pointed out by Chapman and Zwicky [2] , firewalls are an excellent place to focus security decisions and to enforce a network security policy. They are able to efficiently log internetwork activity, and limit the exposure of an organization.

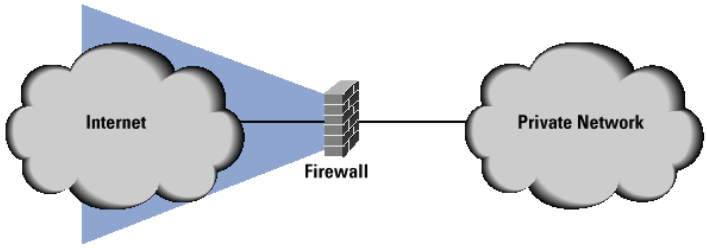
The exposure to attack is called the "zone of risk." If an organization is connected to the Internet without a firewall (Figure 2), every host on the private network can directly access any resource on the Internet. Or to put it as a security officer might, every host on the Internet can attack every host on the private network. Reducing the zone of risk is better. An internetwork firewall allows us to limit the zone of risk. As we see in Figure 3, the zone of risk becomes the firewall system itself. Now every host on the Internet can attack the firewall. With this situation, we take Mark Twain's advice to "Put all your eggs in one basket and watch that basket."

Figure 2: Zone of Risk for an Unprotected Private Network




*Note:Click above for larger view

Figure 3: Zone of Risk with a Firewall




*Note:Click above for larger view

What a Firewall Cannot Do

Firewalls are terrible at reading people's minds or detecting packets of data with "bad intent." They often cannot protect against an insider attack (though might log network activity, if an insider uses the Internet gateway in his crime). Firewalls also cannot protect connections that do not go through the firewall. In other words, if someone connects to the Internet through a desktop modem and telephone, all bets are off. Firewalls provide little protection from previously unknown attacks, and typically provide poor protection against computer viruses.

Firewalls Today: Additions

The first add-on to Internet firewalls was strong user authentication. If your security policy allows access to the private network from an outside network, such as the Internet, some kind of user authentication mechanism is required. User authentication simply means "to establish the validity of a claimed identity." A username and password provides user authentication, but not strong user authentication. On a nonprivate connection, such as an unencrypted connection over the Internet, a username and password can be copied and replayed. Strong user authentication uses cryptographic means, such as certificates, or uniquely keyed cryptographic calculators. These certificates prevent "replay attacks" where, for example, a username and password are captured and "replayed" to gain access. Because of where it sits on both the "trusted" and "untrusted" networks and because of its function as a controlled gateway, a firewall is a logical place to put this service.

The next add-on to Internet firewalls was firewall-to-firewall encryption, first introduced on the ANS InterLock Firewall. Today, such an encrypted connection is known as a Virtual Private Network, or VPN. It is "private" through the use of cryptography. It is "virtually" private because the private communication flows over a public network the Internet, for example. Although VPNs were available before firewalls via encrypting modems and routers, they came into common use running on firewalls. Today, most people expect a firewall vendor to offer a VPN option. Firewalls act as the endpoint for VPNs between the enterprise and mobile users or telecommuters, keeping communication confidential from notebook PC, home desktop, or remote office.

In the past two years, it has become popular for firewalls to also act as content screening devices. Some

additions to firewalls in this area include virus scanning, URL screening, and key word scanners (also known in U.S. government circles as "guards"). If the security policy of your organization mandates screening for computer viruses and it should it makes sense to put such screening at a controlled entry point for computer files, such as the firewall. In fact, standards exist for plugging antivirus software into the data flow of the firewall, to intercept and analyze data files. Likewise, URL screening firewall controlled access to the World Wide Web-and content screening of files and messages seem like logical additions to a firewall. After all, the data is flowing through the fingers of the firewall system, so why not examine it and allow the firewall to enforce the security policies of the organization? The downside to this scenario is performance. Also virus scanning must ultimately be performed on each desktop because data may come in to the desktops from paths other than through the firewall-for instance, the floppy.

Recently, some firewall and router vendors have been making the case for a relatively new firewall add-on called "flow control" to deliver Quality of Service (QoS). QoS, for example, can limit the amount of network bandwidth any one user can take up, or limit how much of the network capacity can be used for specific services (such as FTP or the Web). Once again, because the firewall is the gateway, it is the logical place to put a QoS arbitrating mechanism.

Firewalls Tomorrow

In 1997, The Meta Group, and others, predicted that firewalls would be the center of network and internetwork security [7] . After all, firewalls were the first big security item, the first successful Internet security product, and the most visible security device. They quickly became a "must have" this is good and a "good enough" this is not good because firewalls alone are not sufficient. Firewalls became synonymous with security, as mentioned above. The firewall console becoming the network security console seemed natural at that time. But this scenario has not happened, nor will it happen. The reason? The firewall is just another mechanism used to enforce a security policy. This specific enforcement device will not be the policy management device.

As organizations broaden the base of measures and countermeasures used to implement a comprehensive network and computer security policy, firewalls will need to communicate with and interact with other devices. Intrusion detection devices running on or separate from the firewall must be able to reconfigure the firewall to meet a new perceived threat (just as dynamic filtering firewalls today "reconfigure" themselves to meet the needs of a user).

Firewalls will have to be able to communicate with network security control systems, reporting conditions and events, allowing the control system to reconfigure sensors and response systems. A firewall could signal an intrusion detection system to adjust its sensitivity, as the firewall is about to allow an authenticated connection from outside the security perimeter. A central monitoring station could watch all this, make changes, react to alarms and other notifications, and make sure that all antivirus software and other content screening devices were functioning and "up to rev." Some products have started down this path already. The Intrusion Detection System (IDS) and firewall reconfiguration of network routers based on perceived threat is a reality today. Also, firewall resident IDS and help-desk software enable another vendor's system to expand from a prevention mechanism into detecting and responding. The evolution continues and firewalls are changing rapidly to address the next 100 (Internet) years.

In June 1994, the author wrote [5] , "Firewalls are a stopgap measure needed because many services are developed that operate either with poor security or no security at all." This statement is erroneous. Firewalls are not a stopgap measure. Firewalls play an important part in a multilevel, multilayer security strategy. Internet security firewalls will not go away, because the problem firewalls address-access control and arbitration of connections in light of a network security policy will not go away.

As use of the Internet and internetworked computers continues to grow, the use of Internet firewalls will grow. They will no longer be the only security mechanism, but will cooperate with others on the network. Firewalls will morphas they have from what we recognize today, just as walls of brick and mortar were eventually replaced by barbed wire, motion sensors, and video cameras and brick and mortar. But Internet firewalls will continue to be a required part of the methods and mechanisms used to enforce a corporate security policy. References

1. Avolio, F. and Ranum, M., "A Network Perimeter with Secure External Access," Proceedings of the ISOC NDSS Symposium, 1996. (http://www.avolio.com/papers/isoc.html )

2. Chapman, D. B. and Zwicky, E., Building Internet Firewalls, ISBN 1-56592-124-0, O'Reilly and Associates, 1995.
3. Cheswick, W. and Bellovin, S., Firewalls and Internet Security: Repelling the Wily Hacker, ISBN 0201633574, Addison-Wesley, 1994.
4. Ranum, M. and Avolio, F., "A Toolkit and Methods for Internet Firewalls," Proceedings of the summer USENIX conference, 1994. (http://www.avolio.com/papers/fwtk.html )
5. Shimomura, T. and Markoff, J., Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It, ISBN 0-7868-89136, Warner Books, 1996.
6. Stoll, C., The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage, ISBN 0671726889, Reprint edition, Pocket Books, 1995.
7. Meta Global Networking Strategies File 549, November 24, 1997.

**FREDERICK M. AVOLIO** is an independent security consultant. He has lectured and consulted on Internet gateways and firewalls, security, cryptography, and electronic mail configuration for both government and industry, working in the UNIX and TCP/IP communities since 1979. He is a top-rated speaker and contributor to NetWorld+Interop, USENIX, SANS, TISC, and other security-related forums. With Paul Vixie, Avolio wrote the book Sendmail: Theory and Practice, published by Digital Press. He has an undergraduate degree in Computer Science from the University of Dayton and a Master of Science from Indiana University. E-mail: fred@avolio.com