Firewall Technologies

Gheorghe DODESCU, Bucharest, Romania

Internet provides access to information and the ability to publish information in a revolutionary way. It is also a major danger that provides the ability to pollute and destroy information. A firewall is a form of protection that allows a network to connect to the Internet while maintaining a degree of security. In the paper we will describe the basics of firewalls and summarize what they can do and cannot do to help make sites secure.
Keywords: *firewall, Internet, networks, intrusion.*

Introduction

A firewall is basically a proactive device. When building a firewall, the first thing you need to worry about is what you are trying to protect. When connecting to Internet, there are three things that are put to risk:

- Data: the information kept in the computer
- Resources: the computers themselves
- Reputation

Data has three characteristics that need to be protected:

- Secrecy: one might not want other people to know it
- Integrity: one probably don't want other people to change it
- Availability: one almost certain want to be able to use it himself

Computing resources costs time and money so it is normal that the owner should have o good view on how those resources are used. Intruders often argue that they are using only excess resources so the intrusion won't cost their victims anything. There are two problems with this argument:

- It is impossible for an intruder to determine successfully what resources are in excess and use only those.
- Computer resources are not natural resources, nor are limited resources that are wasted or destroyed if they are not used.

Reputation can be easily affected by intruders who appear on Internet with others' identity. Anything they do appear as if it comes from the victim. Sometimes this costs a lot more than lost time. It shakes people's confidence in the organization.

2. Characteristics of the Internet Firewalls

Firewalls are a very effective type of network security. Theoretically speaking, it prevents the danger of Internet from spreading to your internal network. It serves multiple purposes:

- Restricts people/processes to enter in the system
- Prevents attackers from getting close to the others defenses
- Restricts the way that data that exit the system.

An Internet firewall is most often installed at the point where the protected internal network connects to the Internet. All traffic coming from the Internet or outgoing out from your Internet network passes through the firewall. The firewall has the opportunity to make sure that this traffic is acceptable. This means that whatever is being done – mail, file transfers, remote logins or any kind of specific interactions between specific systems- conforms to the security policy of the site. The policies are different for every site: some are highly restrictive and others are fairly open.

Logically a firewall is a separator, restrictor or analyzer. The physical implementation varies from site to site. Most often, a firewall is a set of hardware components: a router, a host computer or some combinations of routers, computers and networks with appropriate software. There are various ways to configure this equipment. The configuration depends upon the site's security policy, budget and overall operations.

3. Benefits Firewall Usage

So how does one obtain management support for implementation of a firewall? The security practitioner can point out the protection that a firewall provides: protection of the organization's network from intruders, protection of external networks from intruders within the organization, and protection from "due care" lawsuits. But the security practitioner can also list the positive benefits a firewall can provide:

- Increased ability to enforce network standards and policies. Without a firewall or similar device, it is easy for users to implement systems that the Information Services (IS) department doesn't know about, that are in violation of organizational standards or policies, or both. In contrast, organizations find it very easy to enforce both standards and policies with a firewall that blocks all network connections by default. Indeed, it is not uncommon for organizations to discover undocumented systems when they implement such a firewall for the first time.
- Centralized internetwork audit capability. Since all or most traffic between the two networks must pass through the firewall, the firewall is uniquely situated to provide audit trails of all connections between the two networks. These audit trails can be extremely useful for investigating suspicious network activity, troubleshooting connectivity problems, measuring network traffic flows, and even investigating employee fraud, waste, and abuse.

4. Limitations of Firewall Usage

But even with all of these benefits, firewalls still have their limitations. It is important that the security practitioner understand these limitations because if these limitations allow risks which are unacceptable to management, it is up to the security practitioner to present additional safeguards to minimize these risks. The security practitioner must not allow management to develop a false sense of security simply because a firewall has been installed.

- Firewalls provide no data integrity. It is simply not feasible to check all incoming traffic for viruses. There are too many file formats, and often files are sent in compressed form. Any attempt to scan incoming files for viruses would severely degrade performance. Firewalls have plenty of processing requirements without taking on the additional responsibility of virus detection and eradication.
- Firewalls don't protect traffic that is not sent through them. Firewalls can not protect against unsecured, dial-up modems attached to systems inside the firewall; against internal attacks; against social engineering attacks; or against data that is routed around them. It is not uncommon for an organization to install a firewall, then pass data from a legacy system around the firewall because their firewall did not support the existing system.
- Firewalls may not protect anything if they have been compromised. Although this statement should be obvious, many security practitioners fail to educate senior management on its implications. All too often senior management approves - either directly or through silence - a security posture which positively lacks an internal security policy. Security practitioners cannot allow perimeter security via fire walls to become a substitute for internal security.
- Firewalls cannot authenticate datagrams at the transport or network layers. A major security problem with the TCP/IP protocol is that any machine can forge a packet claiming to be from another machine. This means that the firewall has literally no control over how the packet was created. Any authentication must be supported in one of the higher layers.
- Firewalls provide limited confidentiality. Many firewalls have the ability to encrypt connections between two firewalls (using a so-called "virtual private network" or "VPN"), but they typically require that the firewall be manufactured by the same vendor.

A firewall is no replacement for good host security practices and procedures. Individual system administrators still have the primary

responsibility for preventing security incidents.

5. Conclusions

A firewall can only reduce the risk of a breach of security; the only guaranteed way to prevent a compromise is to disconnect the network and physically turn all machines off. Moreover, a firewall should always be viewed as a supplement to host security; the primary security emphasis should be on host security. Nonetheless, a firewall is an important security device which should be used whenever an organization needs to protect one network from another.

References

[Bish03] Bishop, M. - *Computer Security Art and Science*, Ed. Addison-Wesley, 2003

[Pfle03] Pfleeger, C. - *Security in Computing,* Ed. Prentice Hall, 2003

[Ghos01] Ghosh, A. - *Security and Privacy for E-Business,* Ed. John Wiley & Sons, 2001

[BaKa02] Basworth, S., Kabay, M. - *Computer Security Handbook – 4th Edition*, Ed. John Wiley and Sons, 2002.

[TiKr02] Tipton, H., Krause, M. - *Information Security Management - Handbook 4th edition*, Ed. Auerbach, 2002;