DATA SECURITY MANAGEMENT

FIREWALL MANAGEMENT AND INTERNET ATTACKS

Jeffery J. Lowder

INSIDE

Laying the Groundwork for a Firewall; Firewalls and the Local Security Policy; Firewall Evaluation Criteria; Firewall Techniques; Developing a Firewall Policy and Standards; Firewall Standards; Legal Issues Concerning Firewalls; Firewall Contingency Planning

Network connectivity can be both a blessing and a curse. On the one hand, network connectivity can enable users to share files, exchange e-mail, and pool physical resources. Yet network connectivity can also be a risky endeavor if the connectivity grants access to would-be intruders. The Internet is a perfect case in point. Designed for a trusted environment, many contemporary exploits are based on vulnerabilities inherent to the protocol itself. According to a recent dissertation by John Howard on Internet unauthorized access incidents reported to the Computer Emergency Response Team (CERT), there were 4567 incidents between 1989 and 1996, with the number of incidents increasing each year at a rate of 41 to 62 percent. In light of this trend, many organizations are implementing firewalls to protect their internal network from the untrusted Internet.

LAYING THE GROUNDWORK FOR A FIREWALL

Obtaining management support for a firewall prior to implementation can be very useful after the firewall is implemented. When a firewall is implemented on a network for the first time, it will almost surely be the source of many complaints. For example:

- Organizations that have never before had firewalls almost al-

PAYOFF IDEA

Many people incorrectly believe that a firewall is a panacea for their network security concerns; many more believe that they have configured their firewalls correctly when, in fact, they have not. This article addresses the security issues specific to firewall management: choosing a firewall, how to lay the groundwork for a firewall, implementing a firewall, conducting firewall operations, and establishing and enforcing firewall policy and standards.

ways do not have the kind of documentation necessary to support user requirements.
- If the firewall hides information about the internal network from the outside network, this will break any network transactions in which the remote system uses an access control list and the address of the firewall is not included in that list.
- Certain types of message traffic useful in network troubleshooting (e.g., PING, TRACEROUTE) may no longer work.

All of these problems can be solved, but the point is that coordination with senior management *prior to* installation can make life much easier for firewall administrators.

Benefits of Having a Firewall

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. 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 does not 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.* Because all or most traffic between the two networks must pass through the firewall (see below), 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.

Limitations of a Firewall

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 that 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 manage-

ment 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 do not protect traffic that is not sent through it.* Firewalls cannot protect against unsecured, dial-up modems attached to systems inside the firewall; internal attacks; social engineering attacks; or 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 its 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 that positively lacks an internal security policy. Security practitioners cannot allow perimeter security via firewalls 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 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.

FIREWALLS AND THE LOCAL SECURITY POLICY

Cheswick and Bellovin (1994) define a firewall as a system with the following set of characteristics:

- All traffic between the two networks must pass through the firewall.
- Only traffic that is authorized by the local security policy will be allowed to pass.
- The firewall itself is immune to penetration.

Like any security tool, a firewall merely provides the capability to increase the security of the path between two networks. It is the responsibility of the firewall administrator to take advantage of this capability; and no firewall can guarantee absolute protection from outside attacks. The risk analysis should define the level of protection that can be expected from the firewall; the local security policy should provide general guidelines on how this protection will be achieved; and both the assessment and revised policy should be accepted by top management prior to firewall implementation.

Despite the fact that, according to Atkins et al.,[1] all traffic between the two networks must pass through the firewall, in practice this is not always technically feasible or convenient. Network administrators supporting legacy or proprietary systems may find that getting them to communicate through the firewall may not be as easy as firewall vendors claim, if even possible. And even if there are no technical obstacles to routing all traffic through the firewall, users may still complain that the firewall is inconvenient or slows their systems down. Thus, the local security policy should specify the process by which requests for exceptions[1] will be considered.

As Bellovin[2] states, the local security policy defines what the firewall is supposed to enforce. If a firewall is going to allow only authorized traffic between two networks, then the firewall has to know what traffic is authorized. The local security policy should define "authorized" traffic, and it should do so at a somewhat technical level. The policy should also state a default rule for evaluating requests: either all traffic is denied except that which is specifically authorized, or all traffic is allowed except that which is specifically denied.

Network devices that protect other network devices should themselves be protected against intruders. (If the protection device were not secure, intruders could compromise the device and then compromise the system[s] that the device was supposed to protect.)

FIREWALL EVALUATION CRITERIA

Choosing the right firewall for an organization can be a daunting task, given the complexity of the problem and the wide variety of products from which to choose. Yet the following criteria should help the security practitioner narrow the list of candidates considerably.

- *Performance.* Firewalls always impact the performance of the connection between the local and remote networks. Adding a firewall creates an additional hop for network packets to travel through; if the firewall must authenticate connections, that creates an additional delay. The firewall machine should be powerful enough to make these delays negligible.

- *Requirements support.* A firewall should support all of the applications that an organization wants to use across the two networks. Virtually all firewalls support fundamental protocols like SMTP, Telnet, FTP, and HTTP; strong firewalls should include some form of circuit proxy or generic packet relay. The security practitioner should decide what other applications are required (e.g., Real Audio, VDOLive, S-HTTP, etc.) and evaluate firewall products accordingly.
- *Access control.* Even the simplest firewalls support access control based on IP addresses; strong firewalls will support user-based access control and authentication. Large organizations should pay special attention to whether a given firewall product supports a large number of user profiles and ensure that the firewall can accomodate increased user traffic.
- *Authentication*. The firewall must support the authentication requirements of the local security policy. If implementation of the local security policy will entail authenticating large numbers of users, the firewall should provide convenient yet secure enterprisewide management of the user accounts. Some firewalls only allow the administrator to manage user accounts from a single console; this solution is not good enough for organizations with thousands of users who each need their own authentication account. Moreover, there are logistical issues that need to be thought out. For example, suppose the local security policy requires authentication of all inbound telnet connections. How will geographically separated users obtain the proper authentication credentials (e.g., passwords, hard tokens, etc.)?
- *Physical security.* The local security policy should stipulate the location of the firewall, and the hardware should be physically secured to prevent unauthorized access. The firewall must also be able to interface with surrounding hardware at this location.
- *Auditing.* The firewall must support the auditing requirements of the local security policy. Depending on network bandwidth and the level of event logging, firewall audit trails can become quite large. Superior firewalls will include a data reduction tool for parsing audit trails.
- *Logging and alarms.* What logging and alarms does the security policy require? If the security policy dictates that a potential intrusion event trigger an alarm and mail message to the administrator, the system must accommodate this requirement.
- *Customer support.* What level of customer support does the firewall vendor provide? If the organization requires 24-hour-a-day, 365-days-a-year technical support, is it available? Does the vendor provide training courses? Is self-help online assistance, such as a Web page or a mailing list, available?
- *Transparency.* How transparent is the firewall to the users? The more transparent the firewall is to the users, the more likely they will be to

known as the "smurf" attack because of a hacker tool called "smurf," which enables the hacker to launch this attack with relatively little networking knowledge.

Like the SYN attack, the PING Flood Attack relies on IP Source Address Spoofing to add another level of indirection to the attack. In a SYN attack with IP Source Address Spoofing, the spoofed source address receives all of the replies to the PING requests. While this does not cause an overflow on the victim machine, the network path from the bounce site to the victim becomes congested and potentially unusable. The bounce site may suffer for the same reason.

There are automated tools that allow attackers to use multiple bounce sites simultaneously. Attackers can also use tools to look for network routers that do not filter broadcast traffic and networks where multiple hosts respond.

Solutions include:

- disabling IP-directed broadcasts at the router
- configuring the operating system to prevent the machine from responding to ICMP packets sent to IP broadcast addresses
- preventing IP source address spoofing by dropping packets that contain a source address for a different network

CONCLUSION

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 off all machines. 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 that should be used whenever an organization needs to protect one network from another.

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. government."

Notes

1. Atkins, Derek et al. *Internet Security Professional Reference*, 2nd edition, New Riders, Indianapolis, IN, 1997.
2. Bellovin, Steven M. *Security Problems in the TCP/IP Protocol Suite, Computer Communications Review*, 19:2, April 1989, pp. 32–48. Available on the World Wide Web at ftp://ftp.research.att.com/dist/-internet_security/ipext.ps.Z

References

Bernstein, Terry, Anish B. Bhimani, Eugene Schultz, and Carol Siegel. *Internet Security for Business*, John Wiley & Sons, New York, 1996.
Cheswick, W.R. and Bellovin, S.M. *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, Reading, MA, 1994.
Garfinkel, Simson and Spafford, Gene. Practical Unix & Internet Security, Sebastopol, CA, 1995.
Huegen, Craig A. The Latest in Denial of Service Attacks: 'Smurfing', Oct. 18, 1998. Available on the World Wide Web at http://www.quadrunner.com/~chuegen/smurf.txt.

Howard, John D. An Analysis of Security Incidents on the Internet 1989–1995, Ph.D. dissertation, Carnegie Mellon University, Pittsburgh, PA, 1997.
Morris, Robert T. A Weakness in the 4.2BSD Unix TCP/IP Software, *Bell Labs Computer Science Technical Report #117*, Feb. 25, 1985. Available on the World Wide Web at ftp://ftp.research.att.com/-dist/internet_security/117.ps.Z.
Wood, Charles Cresson. Policies from the Ground Up, *Infosecurity News*, March/April 1997, pp. 24-29.

Jeffrey J. Lowder is chief of network security element at the United States Air Force Academy, Colorado Springs, CO.