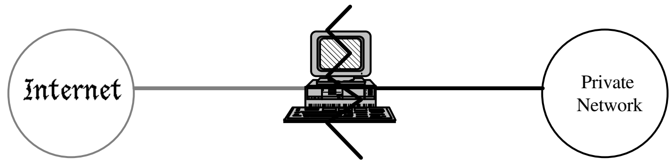
Internet Firewalls
An Overview



Background:

The timely exchange of computerized information is critical to all commercial and government organizations. Local Area Networks and Wide Area Networks form global links that make possible the computer-to-computer exchange of important files, data, and other information. However, the links that connect networks can also be exploited to gain unauthorized access to sensitive or proprietary information.

The Problem:

To provide access between an outside, untrusted network, and an inside, private network. The private network contains proprietary or sensitive data. The outside is untrusted. Valid users outside may be employees at remote sites or local employees who are traveling, or clients and customers who have legitimate reasons to access the private network. Also on the outside, attackers will try whatever they can to gain access to and compromise the data, services, and level of trust on the inside network.

The Solution:

An internetwork *firewall*. Firewalls protect a private network against intrusion by unauthorized users, and they prevent unnoticed and unauthorized export of proprietary information by insiders. "... firewalls span a continuum between ease of use and security.... The rationale for installing a firewall is almost always to protect a private network against intrusion. In most cases, the purpose of the firewall is to prevent unauthorized users from accessing computing resources on a private network, and often to prevent unnoticed and unauthorized export of proprietary information."[1]

The Approach:

There are two basic philosophies that dictate how one configures a firewall: "That which is not expressly prohibited is permitted," and "That which is not expressly permitted is prohibited." In taking the latter approach, all services are blocked, and then individually added after a careful assessment of need and risk. This minimalist approach presents the minimum zone of attack to "the outside." It is more "fail safe," since it accepts that the administrator is ignorant of which network paths are safe, or what security hole may exist in a vendor's operating system or application programs. This approach is also reductionist in its methods, bringing the possible attack points down to as low a number as possible, within the constraints of user requirements and security policies and procedures.

The Services and Components:

As an example of a firewall solution, we look at the TIS Firewall Toolkit components. The firewall toolkit functionality can be broken down into six areas: user authentication, event logging, electronic mail, file transfer,

[1] Marcus Ranum, "Thinking About Firewalls."

remote terminal connections, and other TCP service access control. They provide a manageable, understandable subset of services in a "crystal box"[2] implementation.

User Authentication. The identity of users is established using "challenge/response" systems, which use word lists or special tokens. The computer offers a challenge at login or identification time — a random number, for example, or a word. The user, using a pre-printed word list or a hand-held authenticator, provides the correct response, and is thereby authenticated to the system. This limits the risk from miscreants who are "snooping" on the network; in the case of word pairs, the pair won't be used again, and in the case of a numeric challenge, that particular challenge will never be issued again.

Logging. All significant security events are logged to a protected host on the internal network. This information can be written to disk files, sent to a printer, or both. The logging can be configured for different reactions based on the seriousness of the incident being logged. For example, the software might be configured to call a security manager's beeper in certain instances.

Electronic Mail. Electronic mail is a vital service offered by Internet connectivity, but mailers are one of the favorite points of attack against certain systems. E-mail services are provided in a manner that keeps the private network and the outside network separated, but still allows the exchange of e-mail. Privacy Enhanced Mail (PEM), supporting integrity checking, authentication of the sender, and privacy, can also be part of the firewall solution.

File Transfer. File transfer on the Internet is usually accomplished via the FTP service. The file transfer application gateway is a single process that mediates FTP connections between two networks. It can also be integrated with the user authentication server. Control on a directional,[3] network, host, and user basis can be applied, as well as a tunable audit trail.

Remote Terminal Emulation. The remote terminal connection application gateway is a small, simple, application that mediates TELNET traffic. As with file transfer, this service can be integrated with the user authentication server, and control can be based on direction,[4] network, host, or user.

TCP Access. Most network processes are started up by an initial connection to a general-purpose network listener, which establishes a connection between the incoming request and the program to service the request.[5] The TIS Firewall Toolkit provides access controls that protect TCP-based network services, with the same controls described above for Remote Terminal Emulation and File Transfer.

Summary:

The Internet is a valuable resource, one which will in the coming years continue to change the way people work and communicate on a global scale. The benefits of connection far outweigh the costs, but it is wise to reduce the costs and potential losses as much as possible, by being aware of the dangers and developing appropriate protections.

Trusted Information Systems, Inc., is a world leader in system security assessments and secure network design. TIS can assist system administrators in the design, configuration, installation, and integration of network security components such as firewalls. For further information please send electronic mail to *netsec@TIS.COM*, call (301) 854–6889, Fax to (301) 854–5363, or write to: Trusted Information Systems, Inc., ATTN: Network Security, 3060 Washington Road, Glenwood, MD 21738.

---

[2] Source code of components, security analysis, documentation, and testing available for examination, addition, enhancement, without compromising security.
[3] Both which side of the firewall initiated the process as well as whether files are being copied in or out.
[4] Did the connection initiate inside or outside the firewall?
[5] Picture an old-fashioned telephone switchboard with an operator facing the board.