

Frank Wickham, Senior Systems Engineer, Sun Microsystems

Based on an understanding of Internet risks, an organization can implement any of a number of security architectures. These can incorporate router controls, firewalls, authentication and encryption, and a number of other technologies. An organization should secure both its LAN and its Internet server.

Computer security threats continue to increase. CERT reports a 77% increase in break-ins between 1995 and 1996. Electronic crimes are particularly costly, with a price tag of \$650,000 (compared to \$9,000 for the average bank robbery). Part of the problem is that break-ins often go undetected. One study used common hacker tools to break into Department of Defense systems. 88% of break-ins succeeded. Only 4% were detected.

With the Internet, security policy and technology must reflect distributed computing. More entrances equal more risk. Both host-based (network) security and perimeter (firewall) security are essential. Firewalls should deny all access except that explicitly allowed. Similarly, hosts should provide no services except those explicitly intended.

Firewalls may use a "packet inspection" or "proxy" architecture. In packet inspection, the system picks information off at the datalink layer and filters it against a rules table. Depending on compliance, the system may respond by dropping the incoming packet, passing it through, logging it, sending an acknowledgment, and so forth. In a "proxy" design the security application sits at the top of the OSI stack. Proxy architecture works best with specific services (for example, an FTP server, Telnet server, etc.).

The most common firewall implementation is a double-firewall with a DMZ. In this case, two firewalls bracket a DMZ containing a bastion host. The firewalls should be from different manufacturers, so the same holes do not exist in both.

Firewall security may be extended through one-time password authentication, encryption, stealth (non-IP addressable) machines, packet vectoring, and virtual private networks (VPNs). A VPN uses encryption technology to allow an organization to use a public network as a secure pipeline. This can save 23 to 35% in network costs.

Essential to network security is the configuration of the Internet server. This means limiting the server to required services (for example, FTP), employing a tested recovery plan, frequently checking data integrity, and fully monitoring access. When placing data on an Internet server, an organization must think of the whole world as a potential audience, not just its normal clients. Only a read-only copy of the organization's public information should be accessible.