NATIONAL SECURITY AGENCY

Desktop or Enterprise Firewall?

Deciding upon how much security is necessary always goes back to basic risk analysis. Home users could get by with only desktop firewalls on their personal computers, since the severity of losing data is not that great. Government users on networks connected to the Internet could not rely on desktop firewalls alone since the severity of intrusions would be far too great.

An enterprise firewall will yield the most return on investment for protecting a network. It will protect all internal clients and servers from most external attacks. Those servers that require a different level of external exposure (HTTP, SMTP, etc.) may be placed in a less protected separate (DMZ) network.

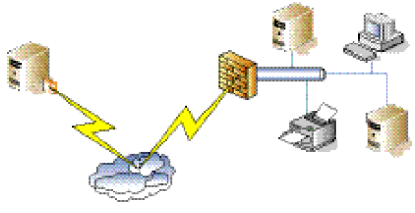
Not all users operate from within the protected network. A mobile user, operating from various locations, cannot feasibly be protected by the enterprise firewall. This is the only time a desktop firewall should be used without an enterprise firewall. The existence and level of acceptable protection for mobile users will rely upon the established Security Policy. Simply put, desktop firewalls offer less protection than an enterprise firewall.

Currently, desktop firewalls are not as sophisticated as enterprise level firewalls. They are limited in their ability to analyze application layer traffic. At best, they only do stateful packet filtering with the addition of binary comparison of applications on the host computer.

What about using *both* a Desktop firewall and an Enterprise firewall?

As with every question involving network security, it is necessary to do some risk analysis before the answer is clear. There must be a cost / benefit analysis done to determine the correct level of protection required.

Adding desktop firewalls to clients within a protected network can provide a substantial improvement to its integrity. With the amount of worms, viruses, "drive by downloads" and whatnot available on the Internet today, let alone targeted malicious attacks, it is inevitable that something will get through the enterprise firewall. Desktop firewalls not only help protect against threats inside the perimeter, but they can also prevent the onward spread of many viruses and worms. For this reason, desktop firewalls that can control both incoming and outgoing traffic are recommended over those that control incoming traffic alone.



Networked Enterprise Firewall

Finally, if a desktop firewall system were to be implemented, it is recommended to employ one where the administrator can push configurations to the desktop. Most organizations lack the personnel or training required to manage the overhead that comes with each user configuring their own desktop firewall, especially since most users do not have the same concerns or awareness of their exposure to the threats that endanger them.

SNAC DoD, 9800 Savage Rd Ft. Meade, MD 20755-6704 410-854-6294 DSN 244-6294 FAX: 410-854-7321 www.nsa.gov/snac