

Firewall Proposal

An easy solution to network security is to use passwords that can't be guessed. Passwords should never be fewer than six characters, someone's name or birth date, an English word, or the word "password."

But good passwords aren't sufficient to protect our network from outside attack. Hackers break into networks to view, alter, or destroy private files. They can also steal passwords. Most security breaches come from the Internet.

A firewall protects the private network from Internet-based attacks. Typical firewalls use rules to block access to certain source/destination addresses. But configuring firewall software is difficult, confusing, and time-consuming.

Packet Filter firewalls are fooled when packet addresses are altered ("IP Spoofing") so the firewall thinks it has an internal (rather than external) source address and grants it network access. This leaves the network open to "Denial of Service" attacks where a server is attacked repeatedly until it crashes. We may have already experienced this situation — our NT servers crash regularly.

Application-level proxy servers examine the network's application layers, leading to slow performance, and require separately configuring the mail and Internet services on the server and each client workstation.

Stateful inspection examines all network layers to accept or reject the requested packet. It is invisible to users and requires no client configuration.

Firewalls that run on a dedicated UNIX or Windows NT server cost from \$3,500 to over \$15,000 and require configuring ability that I don't have. As Windows NT itself isn't secure, I doubt that an NT-based firewall would be secure in the long run. The learning curve to correctly configure a UNIX-based firewall is immense. Cisco and Ascend offer hardware-based costing \$1,500 to \$22,000 but they're also difficult to set up properly.

There's a third choice — Internet Security Appliances.

One in particular — SonicWall (\$995) — appears to meet all our needs. It's easy to set up using an easy web-based interface. It comes preconfigured to detect and stop Denial of Service attacks, IP Spoofing, Ping of Death, SYN Flood, and LAND attacks, all of which are popular on the Internet. It also has Network Address Translation so only one IP address shows over the Internet.

SonicWall was awarded the ICSA FireWall Certification, it works with DSL modems, and it includes free updates as new hacker attacks are discovered. It even logs suspected attacks and sends the network admin an email.