

## The Need for Firewall Protection

The broadband explosion has provided Internet users with a better, faster solution than the traditional dial-up connections we've been used to over the years. That's the good news. The bad news is, broadband connections have some drawbacks, the most serious of which is the fact that they are "always on."

A connection that never shuts off is a hacker's dream. Why? Think of it like this. Would you leave your new sports car unlocked, with the keys in the ignition and the engine running all day long? Not if you don't want it stolen. Hackers like "always-on" connections like DSL, cable modems and T1 lines because they're always there and they're predictable. This isn't to say that broadband connections are bad. Quite the contrary. Broadband is a great technology. Users just need to make sure they're using the appropriate level of protection that a firewall solution can offer.

Hacking, whether it's into your company's network or your personal computer at home, can have serious consequences. For example:

- **Lost Data** - What if someone deleted data on your company's network? What if you didn't have that data backed up? How much would that cost you?
- **Down Time** - Don't you hate it when a customer calls and you have to tell them your server is down? Do you think that customer is going to buy from one of your competitors? Probably.
- **Computer Jacking** - Do you like impersonators? Well, hackers who get control of your computer can launch attacks against other networks using your computer. When the cyber police find out, guess who they're going to be looking for?

Attacks, like those previously mentioned, occur in many forms. Some are minor while others create havoc and do a lot of damage. Here are some others that you need to protect your network against:

- **Denial of Service (DoS)** - Denial of Service attacks are designed to prevent users from accessing a service or resource like a company's public Web site on the Internet.
- **Viruses** - A virus is a computer program that attaches itself to another program and spreads from file to file when that program is run.
- **Worms** - Worms are similar to viruses, except that instead of spreading from file to file, they spread from computer to computer.
- **Trojan Horses** - Like the ancient Greek saga, a Trojan horse is a gift with a little something extra inside. Unfortunately this "gift" usually causes serious problems for your computer.

## Firewall Functionality

Firewalls are a great way to protect your business or home network against attacks from intruders. They're designed to defend against attack by implementing a series of rules that permit, or deny, traffic to pass between your network and the Internet. Based on the way these rules are set, the inbound and outbound flow of information maybe extremely tight or very relaxed. The trick is to maintain a balance between your company's need for security and your employees' need to get their work done without interference.

So what else do firewalls do besides screening email and Web requests? In general, firewalls should have the following functions at a minimum:

- **Stateful Packet Inspection** - Stateful Packet Inspection is a smarter form of packet filtering, which inspects headers of network "packets." It blocks any packet arriving at the firewall claiming to be a solicited response.
- **Network Address Translation (NAT)** - NAT is a technique that hides the IP addresses of your internal computers from prying eyes by replacing them with a single public IP address.
- **Application Proxy** - This service allows firewalls to inspect more than just packet headers before deciding whether or not to allow a packet to pass through.
- **Monitoring and Logging** - Keeping records of attacks is important. It will help you analyze your security needs and provide you with feedback on the performance of your firewall.

As good as firewalls are at defending your network against unwanted intrusions, they can't protect against everything. What threats can't they protect against? Here are a few:

- **Malicious Authorized Users** - These are people on the internal network who are already behind the firewall, which makes this threat difficult to defend against.
- **Social Engineering** - Sometimes hackers obtain information by calling employees and posing as a co-worker or someone else in the company doing a routine check.
- **Viruses, Worms and Trojan Horse Programs** - Firewalls scan network traffic for these threats, however the programs are changing constantly, making them hard to detect.
- **Poor Network Administration** - A firewall is only as effective as its programming. It's up to the network administrator to determine which network traffic should be allowed to pass and which shouldn't.

### **The Sonic WALL Solution**

SonicWALL Internet security appliances are built on stateful inspection firewall technology, the most effective way to protect network access. Stateful inspection technology tracks each packet traversing the firewall and makes sure that they are legitimate. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table ensuring that the source and destination of each packet is valid. This enterprise class technology is designed into every SonicWALL Internet security appliance.

SonicWALL Firewalls:

- Act as a control portal between a protected network and an unsecured network
- Restrict the entrance and exit of traffic based on policies maintained by a network administrator

So far we've talked about how firewalls work, the need for firewall protection and what firewalls can and can't do. Now, let's take a look at your best defense against malicious attacks - the SonicWALL solution. SonicWALL offers a complete line of award-winning Internet Security Appliances (Hardware Firewalls) and Security Applications to protect your customers' networks against attack.

SonicWALL appliances provide secure access to organizations that use the Internet to share confidential information with remote offices, telecommuters, mobile users and partners. No matter what your customers' organizational structure, SonicWALL has the solution to meet their Internet security needs.

SonicWALL's Internet Security Applications provide customers with solutions for integrated Internet security, branch office security and remote access security. Combined with SonicWALL's low total-cost-of-ownership and incredible ease-of-use, these products and integrated applications form a powerful defense against networks attacks.

SonicWALL wall offers your customers a complete security solution by delivering services such as:

- Stateful Packet Inspection Firewall
- Virtual Private Networking (VPN)
- Network Anti-Virus
- Content Filtering
- 8x5 or 24x7 Support Packages!
- Wizard for Easy Installation and Management