

Learn Why Firewall Protection Fails

by Brian A. Reed - Dreaming Tree Technology, Inc. www.Firewalls.com

<http://sonicwall.com/learn-why-fail.asp>

In today's world firewall protection is a must. Without a strong firewall you leave your network vulnerable to many types of worms, trojans and denial of service attacks which translates into lost money.

More often than not, most small businesses buy a firewall, pay an engineer big bucks to configure it and then leave it alone. Proper firewall management is critical to your network security.

Key Reasons Why Firewalls Fail

We have compiled a list of actions that lead to firewall investments becoming worthless or worse, compromised in the small business environment.

- Missing security patches and updates to the firewall equipment
Similar to antivirus programs and computers, security patches and operating system updates must be performed on the firewall. Without properly maintaining the equipment the network's security may become compromised.
- Addition of new computer equipment within the protected environment requiring changes to the firewall
These updates are often added as generic host rules, affecting the security of existing hosts and can result in a vulnerable network. Without a qualified individual to track and make appropriate changes to the firewall can lead to poor network protection.
- Removal of hosts from the infrastructure without the corresponding changes to the firewall policy
This creates a 'leaky' policy firewall which could lead to future hosts on the network to become exposed to the internet in a manner not consistent with the security plan. Without maintaining the firewall policies you run the risk of having your network compromised.
- Addition of 'temporary' policy changes to overcome one-time problems throughout the year
Often a favorite with system administrators, in order to troubleshoot issues with connectivity to the internet, they will create "temporary rules" that bypasses the security provided by the firewall. These "temporary" policies tend to remain in the firewall policy list and are forgotten creating a potential security issue.
- The reviewing of firewall logs becomes less frequent over time
Business owners invest less time monitoring the day-to-day functioning of the firewall and attacks go unnoticed. Without someone constantly analyzing the logs you never know if you are under attack or a network host has been compromised.
- Administration of the firewall changes hands
When an individual stops maintaining a firewall it is typically passed to someone less qualified and less capable of altering the firewall policy. Worse, "temporary policies" and security plan knowledge is never passed on to the next firewall administrator.
- Many people gain rights to administer the firewall
When two or more individuals have admin rights to a firewall no single person knows why certain rules were created in the first place or the significance of a change.

Summary

Most enterprise companies have full-time staff that are available to manage and monitor their firewall. For the other companies it is recommended to hire an outside company to maintain your company's firewall. Working with the right firewall management company can maintain the level of security your network needs while maximizing the investment you made in your firewall.