Firewall

Firewalls are designed to protect individual computers or entire computer networks from unauthorized outside access. They use a set of rules that analyze the origin, destination, content and other parameters of your incoming and outgoing traffic to block unwanted elements.

Why It's On Our Radar

It's just too dangerous of a world out there to leave your network unprotected. By some estimates, an unpatched and unprotected Windows PC connected to the Internet lasts about 20 minutes before being infected by a worm or a virus, or getting compromised in some other way. Security of your corporate information aside, the lack of a strong firewall quite simply means hackers and curious intruders can take control of your network, destabilize your systems and damage your hardware beyond repair. We hate to scare our clients into buying anything, but fear is actually the right motivator to reevaluate the strength of your firewall solution. This is especially true because the cost of good protection is exponentially less than potential costs in downtime, hardware replacement, regulatory fines and lost revenue.

Solution Types

Firewalls can be broadly divided into two categories: software firewalls and hardware firewalls.

Software firewalls are sometimes called "personal firewalls" because they are installed on your personal computer or laptop to protect it from outside attacks. Once the firewall is installed, it must be configured to allow your common connections and applications to run properly. Good personal firewall systems often come as part of broader personal security suites that offer protection against worms, viruses and spam in addition to monitoring traffic. The advantage of personal firewalls is that they are relatively inexpensive and easy to install and configure. The disadvantages are that you have to buy, configure and update firewalls for each computer (this gets bothersome and expensive with more than 5 users), and that a firewall installed on the same machine it's supposed to protect doesn't offer the same measure of security that a separate security device does.

Hardware firewalls make sense for organizations with over five users, or when an office network is in place for servers, file and application sharing, common printers etc.. A hardware firewall usually sits between the office network and the Internet, protecting all computers and servers on the network. This allows you to set a single set of rules and policies for all of your users and makes the firewall easier to manage and update. Hardware firewalls range from simple router-based versions to complex security appliances that include virus scanning, intrusion detection, VPN and other built-in capabilities.

It's important to know that a firewall by itself doesn't provide complete protection for your business, but if it's configured correctly it's a great first step to making your data and your operations secure.

Vendors to Watch

Software firewalls:

- McAfee, Norton, Symantec

Hardware firewalls:

- Cisco ASA 5500,Nokia Checkpoint, SonicWALL, WatchGuard

"U.S. businesses lose $67.2 billion annually to computer-related crime."

FBI

"Most of that is lost by small and medium businesses that think such stats never apply to small and medium businesses."

Bellacom