

A Firewall by any other Name

Contributed by David Conroy
Saturday, 06 January 2007

You called the phone company, ordered up a DSL connection to the internet, and your Internet Service Provider (ISP) tells you they provide a Router and Firewall. But just what is it they are providing? What is the Manufacturer/Model? Does it support VPN connections? Is it secure? Who keeps it patched w/firmware updates?

Your first inquiry into the world of DSL/Cable Modems/T-1 or whatever internet connection you subscribe to (yes, even dial-up) should be in regards to security. To make your life little easier, I will outline some basic facts and correlate them to everyday items so that you can understand what the ISP is talking about.Router

A router is a piece of hardware which will connect you to the ISP network. Typically a router simply acts as a conduit for communications to pass from your computer or network to the outside world. You can liken a router to a highway on-ramp/off-ramp. It provides a clear path for you to send data to or receive data from the "information superhighway" as it used to be called. It simply routes internet traffic to your PC or network based on your internet address (IP Address). It typically does not look at the traffic to limit what comes in or goes out.

A router can be configured with Access Control Lists (ACL) which determine whether or not to allow traffic based on type (i.e.-www, e-mail, etc) or source/destination IP address. While this is a good start, it does not actually look at traffic content to determine whether the traffic is legitimate. NAT

NAT stands for Network Address Translation. Basically, what this means is that your computer's identity is masked by another IP address. You can imagine NAT as sending your child to the market for bread. The grocer simply sees your child, and doesn't know who the bread is actually for. While ISP's will often advertise NAT as a firewall, it is far from it. NAT, like a router, does not look at the traffic content to make sure it is safe. You could very well wind up with moldy bread, since your child is not educated to open the bag, inspect the bread, check its expiration date, and make sure you're getting what you paid for. It's simply making use of a go-between to retrieve and deliver what you want. Firewall

A firewall is a program or piece of hardware which protects your network or computer from other users or networks. It not only will check where traffic comes from, where it is going, and what type it is, but it will make sure that the traffic is properly formatted, and that it was in response to an actual request made by yourself. You can think of the firewall as the security system on your house. It is comprised of various components, such as door locks, keypads, sensors, and cameras, all working together to not only control access, but keep an eye out for suspicious behavior and intruders. A firewall likewise will lock out bad traffic types, allow secure methods for access (through VPN, for example), authenticate users, monitor for suspicious activity and keep a log of everything that happens so that you can trace the source of activity and make you aware of your network's status.

But remember – security is not a solution, it's a process. Buying a piece of hardware is a good first step, but it must be accompanied by maintenance, patching of client pc's, proper security settings on servers, and usage of best-practice principles in regards to passwords and user account settings. If you don't have time, or don't understand what's going on, find a qualified professional to support your needs. Ignorance is what hackers and script kiddies feed on to survive.