Personal Firewalls for Remote Access Users

Date Launched: Aug 12, 2004
Last Updated: Aug 12, 2004
Section: Articles :: Firewalls & VPNs
Author: Deb Shinder
Printable Version
Rating: 3.2/5 - 25 Votes

1 2 3 4 5

Administrators of enterprise level networks often don't pay much attention to the personal firewall market. After all, you need something much more sophisticated to protect your corporate network. But what about the telecommuters and on-the-road executives who connect to your company's network from remote locations? This article looks at how and why you should develop a policy requiring that remote access users have personal firewalls installed – and enabled! – and how to enforce that policy, as well as an overview of some of the personal firewall products available that will do the job at low or no cost.

What's a Personal Firewall and Who Needs One?

The definition of "personal" firewall differs, according to which expert you're listening to. Some equate "personal" with host-based firewalls, while others extend the definition to include off-box firewalls or hardware appliances if they're designed to protect only a single home computer or small network. In the context of this article, we'll use the broader definition and include the low-cost so-called "telecommuter" and "SOHO" appliances offered by many major firewall vendors.

Our point is that *everyone* who connects to your corporate network remotely and who ever also connects that computer to the Internet (by definition, all of your VPN clients and as a practical matter, most likely all of your dial-in remote access clients, too) should have a personal firewall to protect their systems and the networks to which they connect -- especially yours! While your on-site users are behind the corporate firewall, your remote users are exposed to the outside whenever they dial up or plug into their broadband connections.

That's why you need a policy requiring personal firewalls for anyone who wants to connect remotely, whether from a home computer or from a notebook or PDA while on the road (yes, there are firewall software packages for handheld computers; see my article titled *Securing Your Pocket PC* at http://www.windowsecurity.com/articles/Securing-Pocket-PC.html). But it's not enough to simply require that they have a firewall; it must also be *properly configured* and it must be *enabled.* Many home users simply turn their firewalls off or open them up to everything if they have access problems. Your policy should be specific as to how the firewall should be configured and require that it be turned on.

Enforcing Personal Firewall Policy

All that is well and good, but how do you enforce the policy over computers that aren't under your physical control? The best way is via your own corporate firewall or VPN/remote access server. The latest products of most major vendors include a feature that allows you to block connections if the remote client doesn't meet your specified criteria. For example, ISA Server 2004 calls this "VPN Quarantine." Other vendors call it "managed VPN client" or other terms.

Whatever it's called, it's a good thing. One of the criteria you can set is that the clients must have personal firewalls installed and enabled. If they don't, the connection is denied or the client is "quarantined" and disallowed access with most of the internal network. You can set up special servers within the "quarantine" network that these clients *can* access. For example, you can provide a server from which they can download the software they need to install in order to comply with your policies.

To use this feature with most major firewall products, you have to use their proprietary VPN client software. Many vendors offer two VPN clients, a free "basic" one and the "managed" or "security" client that allows you control and also costs you extra. With ISA Server, though, all you need is the VPN software that's already built into modern Windows operating systems. Even without ISA, you can use the network access quarantine control feature of a Windows Server 2003 remote access/VPN server. For more info, see http://www.windowsecurity.com/articles/Server-2003-Network-Access-Quarantine-Control-Securit

Picking a Personal Firewall

Of course, you could just allow your remote users to pick whatever personal firewall they like (after all, any firewall is better than no firewall), but the best practice is to have them all use the same one. After all, you'll probably be called on to support it when they have problems. That's easier to do when their computer hardware is issued by the company. If it belongs to them, you might not be able to tell them what firewall to use – but you *can* prohibit them from connecting to the company network if they don't use the prescribed one.

Choosing the right personal firewall to protect your remote users opens up a wide range of

Choosing the right personal firewall to protect your remote users opens up a wide range of choices. Prices run from free to several hundred dollars. Software firewalls that run on the host computer are less expensive. Some popular choices include:

- **The Windows firewall (formerly known as Internet Connection Firewall or ICF) built into Windows XP**. This choice has a couple of important advantages: it comes with Windows so there's nothing to install, and it doesn't cost extra. It's a pretty rudimentary firewall but sufficient for most home users, and XP Service Pack 2 (SP2) makes some improvements to the firewall (we'll discuss these in detail in a future article).
- **Zone Alarm from Zone Labs**. This has been one of the most popular personal firewalls with consumers for years. Zone Labs (www.zonelabs.com) offers a free basic firewall that can be downloaded from their Web site, but it's only for individuals and non-profits. It's a basic firewall with basic intrusion detection included. For commercial use (and I think they would argue that when an individual connects to your corporate network, it's commercial), the price is $39 for a single user license – a reasonable price for a solid personal firewall product. This also gets you the "Pro" version, which has more functionality and includes automatic program configuration, identity and privacy protection features, and e-mail security. There's an eval version you can try out before you buy.
- **Norton Personal Firewall from Symantec.** Norton's product is also popular with consumers and designed to work in conjunction with their popular anti-virus software. It allows configuration of different firewall settings for different network, something that can be handy for laptops that connect to more than one network. It includes intrusion detection and privacy control, and uses LiveUpdate to automatically check for updates online. List price is $49.95.

Hardware appliances designed to protect telecommuters are more expensive. For example:

- **Linksys** and **Netgear** (among other companies that make networking equipment targeted at home users) offer low-cost firewall/broadband router combo devices for DSL and cable modem users. These are fairly simple; they can block or hide ports, but don't usually include sophisticated intrusion detection or application layer attack protections. Cost is around $200, but also includes the broadband routing functionality.
- **SonicWall** and **Watchguard** offer firewall appliances specifically aimed at telecommuters and small office/home office (SOHO) users. Some of these also can act as VPN gateways. Prices are in the $400-600 range.
- **Cisco's PIX 501** is a low-end appliance firewall and VPN gateway designed for small offices that can be used for telecommuters, especially those who want to protect a small home network. Cost is $500-800 (depending on number of users; for $500 you can get 10 user licenses).
- **NetScreen's** 5 series (5XP, 5XP Elite, 5GT, 5GT Plus, 5XT and 5XT Elite) are appropriate for telecommuters and will protect a small office, also provide VPN gateway functionality. Cost starts at just under $500.

The hardware appliances provide "turn key" solutions. Because they are "off box" (not running on the same computer they're protecting), they don't affect the computer's performance or use its resources. They generally run proprietary operating systems, which makes them harder (though not impossible) to hack.

What if a telecommuter, who has a hardware appliance installed at home, decides to take that laptop on vacation and VPN from the hotel or a relative's house? The hardware appliances are more appropriate for protecting home networks from which your remote users will connect, or desktop systems that stay put. Software firewalls installed on the host are more appropriate for portable systems that may move from one location to another.

Summary

There are a plethora of software- and hardware-based firewall products available that are designed with the telecommuter in mind, and can provide vital protection to the computers that connect to your network via remote access. Your organization should develop a written policy requiring personal firewall protection (and other protections such as anti-virus and up-to-date security patches and service packs) for all remote access clients. You should not rely on users to comply voluntarily, but instead enforce compliances through remote access controls such as Windows Server 2003/ISA Server's quarantine features or the managed client/security client features of other enterprise level firewall vendors. The network you save just might be your own.

About Deb Shinder

Debra LittleJohn Shinder(MCSE) is a technology consultant, trainer and writer who has written a number of books on networking, including Computer Networking Essentials, published by Cisco Press and Scene of the Cybercrime, published by Syngress Media. She is co-author, with her husband Dr. Thomas Shinder, of Troubleshooting Windows 2000 TCP/IP and the best-selling Configuring ISA Server 2000, both published by Syngress Media, as well as the new ISA Server and Beyond. Deb tech edited Syngress's Security + Study Guide and was a major contributor to Que's TruSecure ICSA Certified Security Associate exam guide. Deb lives and works in the Dallas-Ft Worth area and can be contacted at deb@shinder.net or via the website at www.shinder.net.