

By Thomas W Shinder MD, MVP

Microsoft has made security a top priority over the past several years, and many security mechanisms and tools are included with the Windows operating systems and available as free downloadable add-ons. Several of these, however, aren't utilized to their full potential. Here's a look at 10 of the most underappreciated and overlooked Microsoft security technologies.

1 TCP/IP filtering

All versions of Windows 2000 and Windows Server 2003 include a TCP/IP filtering feature that allows you to control what TCP/UDP ports and IP protocols the Windows operating system will accept incoming connections to. You'll find TCP/IP filtering in the Advanced TCP/IP Properties dialog box on the Options tab. You can configure TCP/IP filtering to limit connections to incoming TCP ports, incoming UDP ports, and incoming IP protocols (by specifying the IP protocol number, such as IP protocol number 47 for GRE). TCP/IP filtering applies to all network interfaces on the machine. One limitation of TCP/IP filtering is that it does not allow you to block or control ICMP traffic.

2 Microsoft Certificate Services

A public key infrastructure (PKI) is a vital element in any organization's overall security design. PKI depends on creating and delivering digital certificates that can be used to authenticate machines and users. One option is to use a commercial certificate authority, but this can be an expensive proposition for most corporate networks. If you have Windows 2000 or Windows Server 2003 servers on your network, you can easily create your own Microsoft Certificate Services-based certificate authorities to issue certificates to all the machines and users on your network. You can configure Microsoft Certificate Services to work with Active Directory group policy so you can automatically deploy digital certificates to all managed machines in your Active Directory domain.

3 Windows XP Service Pack 2 Windows Firewall

Microsoft's first attempt at a personal or host-based firewall was the Internet Connection Firewall (ICF). Although ICF was a good first attempt, it lacked flexibility and effective centralized management capabilities. All this changed with the Windows Firewall. The Windows Firewall allows you to block all incoming connections to Windows hosts or to configure exceptions based on application or port number. You can fine-tune the exceptions by allowing connections from a specific network ID or even a specific IP address. The Windows Firewall can also be centrally managed via Active Directory group policy.

4 Microsoft Baseline Security Analyzer (MBSA)

The [Microsoft Baseline Security Analyzer](#) is a free tool you can use to scan Windows client and server systems on your network to discover the current security configuration of those hosts. The MBSA offers an easy-to-use graphical interface that lets you scan one or thousands of computers on your network. You can also use the command-line interface support to schedule scans and keep a comprehensive database.

5 VPN for high security segments

Most network and security administrators think of VPN only as a remote access solution. Although VPN makes a great remote access solution, you can also use it to segregate high security network segments from the rest of the corporate network. For example, is there any reason why users need access to servers and workstations located on the Human Resources network? Yes, a select group of users may require access, but not all users. You can put a Microsoft VPN server at the edge of that network and require users to connect to that network via L2TP/IPSec. L2TP/IPSec requires computer authentication using digital certificates, and you can further enhance the security configuration by requiring user certificate authentication.

6 Group policy software restriction policies

Microsoft group policy software restriction policies allow you to control which programs can run on your computer. For instance, you could create a policy that prevents specific file types from running in the e-mail attachment folder used by your e-mail client if you're concerned about users receiving viruses through e-mail. Or you might allow users to access only specific files on multiuser computers.

Software restriction policies also allow you to control who can add trusted publishers to managed computers, and you can determine whether the policies affect all users or just certain users on a computer. Using software restrictions, you can prevent any files from running on your local computer, your organizational unit, your site, or your domain. For instance, if there is a known virus, you can use software restriction policies to stop the computer from opening the file that contains it.

7 IPSec domain isolation

IPSec domain isolation is a method of controlling traffic between all machines on your Active Directory network. Do client systems really need to be able to connect to one another for any reason? Do all client systems need to connect to all servers on your network? Do all servers, even those in the same security zone, need to connect to one another? Of course not. Although most of us tend to think of IPSec as an encryption methodology, it's less processor intensive and equally effective when not employing encryption. For more information on IPSec domain isolation, check out [Microsoft's comprehensive white paper](#) on the topic.

8 Internet Authentication Server (IAS)

Internet Authentication Server (IAS) is Microsoft's version of RADIUS, which enables you to authenticate users against your Active Directory from machines that are not domain members. It's especially useful for wireless LAN access, remote access VPN connections, and Web proxy client authentication. You can also use IAS remote access policies and apply them to the wireless, VPN, and Web proxy client connections. IAS is part of the Windows Server 2003 operating system and you can install it from the Add/Remove Programs applet.


9 Microsoft Firewall (Winsock proxy) Client

The ISA Server firewall's Firewall Client application is a generic Winsock proxy client application. Unlike SOCKS-based proxies, which require that you configure each SOCKS-compliant application to use them, the Firewall Client automatically intercepts and remotes connections from Winsock applications (almost all networked applications in the Microsoft environment) to the ISA firewall's Firewall service. The Firewall Client forwards user credentials over an encrypted channel, which enables transparent authentication with the ISA firewall and enables strong user/group-based outbound access control. In addition, the Firewall Client forwards the name of the application to the ISA firewall. This enables you to get user name and application names associated with each connection through the ISA firewall, and all this information is available in the firewall's log files and reports.

10 Encrypting File System for laptop security

The Encrypting File System (EFS) allows you to encrypt files, groups of files, directories, or even an entire disk with strong certificate-based encryption. EFS works together with Active Directory and Group Policy to provide strong file-based encryption and over-the-network encryption when accessing files over WebDAV. EFS is especially valuable when deployed on laptop computers, which are much more likely to be stolen. Windows XP includes several improvements that prevent thieves from removing the hard drive from the laptop and resetting the administrator password. EFS is a core data security feature that should be considered on all corporate laptops.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) 
- Sign up for our [Downloads Weekly Update](#) newsletter
- Sign up for our [Network Security NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- "[Verify security settings on Windows XP using Microsoft Baseline Security Analyzer 1.2](#)" (TechRepublic article)
- "[10 reasons to use ISA Server 2004 as your remote access VPN server and VPN gateway](#)" (TechRepublic download)
- "[Build Your Skills: Get acquainted with Windows Server 2003 security features](#)" (TechRepublic article)

Version history

Version: 1.0

Published: January 6, 2006

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team