

By Debra Littlejohn Shinder, MCSE, MVP

Microsoft has made significant changes to the Windows Firewall in Vista that enhance security and make it more configurable and customizable for advanced users, while retaining the simplicity required by novices. Here are some key aspects of the changes.

1 Two interfaces to meet different needs

The Vista firewall has two separate graphical configuration interfaces: a basic configuration interface accessible through the Security Center and Control Panel and an advanced configuration interface accessible as a snap-in when you create a custom MMC. This prevents novice users from inadvertently making changes that could disrupt their connectivity or put them at risk, while providing a way for advanced users to customize firewall settings more granularly and control outbound as well as inbound traffic. You can also use commands in the `netsh advfirewall` context to configure the Vista firewall from the command line or create scripts to automatically configure the firewall on a group of machines. You can also control the Vista firewall settings through Group Policy.

2 Basic configuration options

With the basic configuration interface, you can turn the firewall on or off or set it to block all programs with no exceptions, and you can create exceptions (programs, services, or ports that you specifically unblock) and specify the scope of each exception (whether it applies to traffic from all computers, including those on the Internet, only computers on your local network/subnet, or only computers that you identify by IP address or subnet. Here you can also specify which connections you want the firewall to protect, and configure security logging and ICMP settings.

3 Secure by default

The Windows Firewall in Vista defaults to a secure configuration, while still supporting best usability. By default, most inbound connections are blocked and outbound connections are allowed. The Vista firewall works in conjunction with Vista's new Windows Service Hardening feature, so that if the firewall detects behavior that is prohibited by the Windows Service Hardening network rules, the firewall will block that behavior. The firewall also fully supports a pure IPv6 network environment.

4 ICMP message blocking

By default, incoming ICMP echo requests are allowed through the firewall, and all other ICMP messages are blocked. This is because the Ping tool is routinely used to send echo request messages for troubleshooting purposes. However, hackers can also send echo request messages to locate target hosts. You can block echo request messages (or unblock other ICMP messages if they're needed for diagnostic purposes) through the Advanced tab on the basic configuration interface.

5 Multiple firewall profiles

The Vista Firewall With Advanced Security MMC snap-in allows you to set up multiple firewall profiles on your computer, so that you can have a different firewall configuration for different situations. This is especially useful for portable computers. For example, you may want a more secure configuration when you're connected to a public wi-fi "hotspot" than when you're connected to your home network. You can create up to three firewall profiles: one for connecting to a Windows domain, one for connecting to a private network, and one for connecting to a public network.

6 IPsec features

With the advanced configuration interface, you can customize IPsec settings to specify the security methods to be used for both integrity and encryption, determine the lifetime for keys in minutes and sessions, and select the desired Diffie-Hellman key exchange algorithm. Data encryption for IPsec connections is not enabled by default, but you can enable it and select which algorithms are to be used are data integrity and encryption. Finally, you can select to authenticate the user, computer, or both via Kerberos, require computer certificates from a CA that you specify, or create custom authentication settings.

7 Security rules

A wizard guides you through the steps of creating security rules to control how and when secure connections are to be created between individual computers or groups of computers. You can restrict connections on such criteria as domain membership or health and exempt specified computers from connection authentication requirements. You can set up rules to require authentication between two specific computers (server-to-server) or use tunnel rules to authenticate connections between gateways. You can also create custom rules if none of the predefined rule types is appropriate.

8 Custom authentication rules

When you make a custom authentication rule, you specify individual computers or groups of computers (by IP address or address range) to be the endpoints of the connection. You can either request or require authentication for inbound connections, outbound connections or both. For example, you can require authentication for inbound connections but only request it for outbound connections. When authentication is requested, the connection will be authenticated if possible, but will still be allowed through unauthenticated if it is not.

9 Inbound and outbound rules

You can create inbound and outbound rules to block or allow connections for specific programs or ports. You can use the preconfigured rules or make your own custom rules. The New Rule Wizard guides you through the steps of creating a rule. You can apply a rule to programs, ports or services, and you can have the rule apply to all programs or to a specific program. You can block all connections for that program, allow all connections, or allow only secure connections and require encryption to protect the confidentiality of the data sent over the connection. You can configure both source and destination IP addresses for both inbound and outbound traffic. Likewise, you can configure rules for both source and destination TCP and UDP ports.

10 AD-based rules

You can create rules to block or allow connections based on Active Directory user, computer, or group accounts, as long as the connection is secured by IPsec with Kerberos v5 (which includes the Active Directory account information). You can also use the Windows Firewall With Advanced Security to enforce Network Access Protection (NAP) policy.



Debra Littlejohn Shinder is a technology consultant, trainer and writer who has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP*, the best-selling *Configuring ISA Server 2000*, and *ISA Server and Beyond*.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [Windows Vista Report newsletter](#)
- Check out all of TechRepublic's [free newsletters](#)
- "[Installing Windows Vista: The good, the bad, and the ugly](#)" (TechRepublic download)
- [10 things to consider before rolling out Windows Vista in your organization](#) (TechRepublic download)
- "[Vista's Aero Glass: Is it all it's cracked up to be?](#)" (TechRepublic article)

Version history

Version: 1.0

Published: November 1, 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