

Introduction to Windows Firewall with Advanced Security

Microsoft Corporation

Updated: December 2009

Abstract

Windows® Firewall with Advanced Security is a stateful, host-based firewall that blocks incoming and outgoing connections based on its configuration. While typical end-user configuration of Windows Firewall still takes place through the Windows Firewall Control Panel program, advanced configuration in an enterprise networking environment now takes place in a Microsoft® Management Control (MMC) snap-in named Windows Firewall with Advanced Security. The inclusion of this snap-in not only provides an interface for configuring Windows Firewall locally but also for configuring Windows Firewall on remote computers and via Group Policy. Firewall functions are now integrated with IPsec (Internet Protocol security) protection settings, reducing the possibility of conflict between the two protection mechanisms. Windows Firewall with Advanced Security supports separate profiles for when computers are domain-joined or connected to a private or public network. It also supports the creation of rules for enforcing server and domain isolation policies. Windows Firewall with Advanced Security supports more specific rules, including Microsoft Active Directory® users and groups, source and destination Internet Protocol (IP) addresses, IP port number, ICMP settings, IPsec settings, specific types of interfaces, services, and more.



The information that is contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft Windows Server, Windows 7, Windows Vista, Active Directory, and the Windows logo are either registered trademarks or trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Introduction to Windows Firewall with Advanced Security 5](#_Toc247427932)

[Business and Technical Benefits 6](#_Toc247427933)

[Key Scenarios 6](#_Toc247427934)

[Network Location-Aware Host Firewall 7](#_Toc247427935)

[Server and Domain Isolation 8](#_Toc247427936)

[Network Access Protection 10](#_Toc247427937)

[DirectAccess 10](#_Toc247427938)

[Managing Windows Firewall with Advanced Security 11](#_Toc247427939)

[Order of Windows Firewall with Advanced Security Rules Evaluation 11](#_Toc247427940)

[Managing a Single Computer with the Snap-in 13](#_Toc247427941)

[Configuring Firewall Properties 15](#_Toc247427942)

[Configuring a Profile 15](#_Toc247427943)

[Configuring IPsec Settings 18](#_Toc247427944)

[Viewing Rules 20](#_Toc247427945)

[Creating New Rules 25](#_Toc247427946)

[Creating Connection Security Rules 28](#_Toc247427947)

[Isolation 29](#_Toc247427948)

[Authentication exemption 29](#_Toc247427949)

[Server-to-server 30](#_Toc247427950)

[Tunnel 30](#_Toc247427951)

[Custom 31](#_Toc247427952)

[Using the Netsh Advfirewall Command-Line Tool 31](#_Toc247427953)

[Managing Windows Firewall with Advanced Security by Using Group Policy 32](#_Toc247427954)

[Monitoring Windows Firewall with Advanced Security 33](#_Toc247427955)

[Firewall 33](#_Toc247427956)

[Connection Security Rules 34](#_Toc247427957)

[Security Associations 34](#_Toc247427958)

[Additional Resources 34](#_Toc247427959)

# Introduction to Windows Firewall with Advanced Security

Almost every computer is now connected to a network. The information available from the Internet and stored on our private and corporate networks makes universal network connectivity almost mandatory. The growth of wireless networking options increases our mobility without compromising our access to the information we need.

But with this universal connectivity comes increased risk. The ease of connection that allows authorized users to access resources from almost anywhere at any time can also allow unauthorized users and malicious programs to attack a network with relative speed and anonymity.

Protecting your network and information assets requires a layered, defense-in-depth security model. You must protect the computers on your network from unauthorized users and programs not only on the Internet, but also on the local intranet. A layered defense can provide protection from unauthorized, unmanaged, and noncompliant computers no matter how they connect to the network.

Windows Firewall with Advanced Security is an important part of a layered security model. By providing host-based, two-way network traffic filtering for a computer, Windows Firewall with Advanced Security blocks unauthorized network traffic flowing into or out of the local computer. Windows Firewall with Advanced Security also works with Network Awareness so that it can apply security settings appropriate to the types of networks to which the computer is connected. Now that Windows Firewall and Internet Protocol Security (IPsec) configuration settings are integrated into a single Microsoft Management Console (MMC) named Windows Firewall with Advanced Security, Windows Firewall also becomes an important part of your network’s isolation strategy.

Your feedback is valuable and welcome! Please send your comments and suggestions to Windows Firewall with Advanced Security Documentation Feedback (wfasdoc@microsoft.com). The author of this guide will review your comments and use them to improve this documentation. Your e-mail address will not be saved or used for any other purposes.

In this document:

 [Business and Technical Benefits](#zd9352cf520a24c15ab39a916766a6f45)

 [Key Scenarios](#z829cda76eb8c414d954b1e08c683fa8e)

 [Managing Windows Firewall with Advanced Security](#zf81a8ae3b2794a1bba3ce647f5529c27)

 [Additional Resources](#zaeeca7b0c98a4618860428f27b5fd72a)

# Business and Technical Benefits

Windows Firewall with Advanced Security provides your organization with a scalable and tightly-integrated solution that is also simple to use.

Connected computers face the following challenges:

 Mobile workers and devices complicate a network’s physical topology, making it difficult to prevent unauthorized access to trusted network assets.

 Viruses, worms, and denial of service (DoS) attacks are increasing in complexity, making it more difficult to mitigate the risk of malware and other threats.

 Regulatory burdens are increasing, making it more difficult to achieve and maintain compliance with legislative regulations.

 Data is a critical asset for almost every employee in most organizations, making it difficult to limit access to only authorized users while still providing ease of access.

To help address these challenges, Windows Firewall with Advanced Security offers the following benefits:

 Reduces the risk of network security threats.  Windows Firewall with Advanced Security reduces the attack surface of a computer, providing an additional layer to the defense-in-depth model. Reducing the attack surface of a computer increases manageability and decreases the likelihood of a successful attack. Network Access Protection (NAP), a feature of Windows Server® 2008 R2 and Windows Server® 2008, also helps ensure client computers comply with policies that define the required software and system configurations for computers that connect to your network. The integration of NAP helps prevent communications between compliant and noncompliant computers.

 Safeguards sensitive data and intellectual property.  With its integration with IPsec, Windows Firewall with Advanced Security provides a simple way to enforce authenticated, end-to-end network communications. It provides scalable, tiered access to trusted network resources, helping to enforce integrity of the data, and optionally helping to protect the confidentiality of the data.

 Extends the value of existing investments.  Because Windows Firewall with Advanced Security is a host-based firewall that is included with Windows® 7, Windows Vista®, Windows Server 2008 R2, and Windows Server 2008, and because it is tightly integrated with Active Directory® Domain Services (AD DS) and Group Policy, there is no additional hardware or software required. Windows Firewall with Advanced Security is also designed to complement existing non-Microsoft network security solutions through a documented application programming interface (API).

# Key Scenarios

You can use Windows Firewall with Advanced Security to help implement the following key technologies and scenarios:

 [Network Location-Aware Host Firewall](#ze26edbae84584a2298356ec3f1c8f57a)

 [Server and Domain Isolation](#zbea2b60a5f7c4432997e2daff2f2c5b3)

 [Network Access Protection](#z69ce79c61ac6409eb9bfbbd9c0daddd1)

 [DirectAccess](#z0860fecb0ea34390bf7f195e50ee1d60)

# Network Location-Aware Host Firewall

Many applications connect to the Internet to look for updates, download real-time information, and facilitate collaboration between users. However, creating applications that can automatically adapt to changing network conditions has been difficult for developers. Windows 7, Windows Vista, Windows Server 2008 R2 and Windows Server 2008 alert applications to changes in the detected network connectivity, and applications can then operate differently to provide a seamless experience.

Windows identifies and remembers each of the networks to which it connects. Network Awareness application programming interfaces (APIs) then allow applications to query for characteristics of each of these networks, including:

 Connectivity.  A network might be disconnected, it might provide access to the local network, the Internet, a corporate network, or any combination of the three.

 Connections.  The computer might be connected to a network through one or more connections. Network Awareness APIs enable applications to determine which connections the computer is currently using to access a given network.

 Location.  Each network is assigned a location that identifies its type. Some of the operating system settings change based on the location of the networks to which it is connected. For example, Windows Firewall with Advanced Security can enforce different policies based on the locations of the networks to which the computer is currently connected.

There are three categories of network locations in Windows:

 Domain.  The Windows operating system automatically identifies networks on which the computer can authenticate access to a domain controller for the domain to which the computer is joined. You cannot manually assign a network to this location.

 Public.  With the exception of domain networks, all networks are initially categorized as public. Networks that represent direct connections to the Internet or that are in public places, such as airports and coffee shops, should be left public.

 Private.  A network will be categorized as private only if a user or application designates it as private. Only networks located behind a private gateway device should be designated as private networks. Users will likely want to designate home or small business networks as private.

When a user connects to a network that is not identifiable as a Domain location, Windows asks the user to designate the network as either Public or Private. The user must be a local administrator of the computer to designate the network as Private. When the type of network to which the computer is connected is identified, Windows can optimize some of its configuration, especially its firewall configuration, for the specified network location.

Windows Firewall with Advanced Security is an example of a network-aware application. The administrator can associate a profile to each network location, with each profile containing different firewall policies. For example, Windows Firewall can automatically allow incoming traffic for a specified desktop management tool when the computer is on a domain network but block that same traffic when the computer is connected to a public or private network. In this way, Network location awareness can provide flexibility on your internal network without sacrificing security when mobile users travel. The Network Location Awareness APIs complement the robust and flexible filtering built into Windows Firewall with Advanced Security, which lets you filter programs, services, or ports for IP address scopes, interface types, users, groups, computers, and levels of protection – all based on which network locations to which the computer is connected. A public network profile should have stricter firewall policies to protect against unauthorized access. A private network profile, on the other hand, might have less restrictive firewall policies to allow file and printer sharing, peer-to-peer discovery, and connectivity with Windows Connect Now devices. Domain profiles typically have the least restrictive rules, because the computers on that network are trusted.

 Windows Vista and Windows Server 2008 support only a single profile on the computer at a time. If the computer is connected to more than one network, then the network location that requires the most protection is the one applied to all connections on the computer. If a public network is detected, then all connections to the computer are protected by the rules associated with the public profile. If a private network is detected and there are no public networks detected, then the private profile is applied to the computer. Only if a domain network is detected and there are no public or private networks detected is the domain profile applied.

 Starting with Windows 7 and Windows Server 2008 R2, Windows supports a separate profile for each network connection. If a connection to a public network is detected, then that connection is protected by the rules associated with the public profile. A connection to a domain network on the same computer is protected by the domain profile. All of the profiles can be active at the same, each protecting the connections according to its network location type.

By default, unsolicited incoming traffic is blocked. You must create rules to allow other authorized traffic to pass through the firewall into the computer. The default settings allow all outgoing traffic. You must specifically block programs or types of traffic that should not be allowed.

You will learn how to configure these profiles and create rules in the section [Managing Windows Firewall with Advanced Security](#zf81a8ae3b2794a1bba3ce647f5529c27).

# Server and Domain Isolation

In a Windows-based network, you can logically isolate server and domain resources to limit access to authenticated and authorized computers. For example, you can create a logical network inside the existing physical network where computers share a common set of requirements for secure communications. Each computer in this logically isolated network must provide authentication credentials to other computers in the isolated network in order to establish connectivity. Network traffic from computers and users that either cannot authenticate, or that authenticate as a computer or user that is not on the authorized list, is dropped. This isolation prevents unauthorized computers and programs from gaining access to resources.

Server and domain isolation can help protect high-value servers and data as well as protect managed computers from unmanaged or rogue computers and users.

You can use two types of isolation to protect a network:

 Server isolation.  In this scenario, a server is configured with IPsec connection security rules that require communications from other computers to be both authenticated and authorized, and optionally encrypted. For example, you might configure the database server to accept connections from the Web application server only. Another common scenario is to protect the sensitive payroll servers by restricting them to accepting communications only from computers that can authenticate as an authorized member of the payroll client computer group.

 Domain isolation.  To isolate a domain, you use Active Directory domain membership as criteria in connection security rules to ensure that domain-member computers accept only authenticated communications from other domain-member computers. Communications from non-domain members are dropped. You can create exception rules that permit unauthenticated communications from specific non-domain member computers. The isolated network consists only of computers that are part of the domain, as shown in Figure 1.

Figure 1. Protecting network computers with domain isolation



For more information about server and domain isolation, see [Server and Domain Isolation](http://go.microsoft.com/fwlink/?linkid=95395) (http://go.microsoft.com/fwlink/?linkid=95395).

# Network Access Protection

Network Access Protection (NAP) is a technology available in Windows 7, Windows Vista, Windows Server 2008 R2, and Windows Server 2008. NAP enforces health requirements on client computers that are attempting to connect to a network. Health requirements can include items like ensuring that the client is configured with up-to-date antivirus protection, and that all of the available critical security updates have been installed.

NAP includes client and server components that allow you to create and enforce health requirement policies that define the required software and system configurations for computers that connect to your network. When NAP determines that a client does not comply with the health requirements, NAP helps to protect other computers on the network by restricting network access for non-compliant computers. Typically, access for non-compliant computers is limited to only those servers that can provide remediation, such as a Windows Server Update Services (WSUS) server, or a server that can provide updated antivirus definition files. NAP does not allow unlimited network access until the client computer has been brought back into compliance.

NAP can use Windows Firewall with Advanced Security to enforce policy as part of a larger isolation strategy. Typically, NAP is implemented in a manner similar to an isolated domain, but requires computer certificates instead of Active Directory domain-based Kerberos for authentication. Only computers that are determined to be “healthy” are provisioned with the computer certificate that is required to authenticate. Network traffic from computers that are not “healthy” is dropped. Servers that can provide remediation by providing antivirus updates or the latest security updates are the only computers that are configured to accept unauthenticated traffic.

For more information about NAP, see [Network Access Protection](http://go.microsoft.com/fwlink/?linkid=111066) (http://go.microsoft.com/fwlink/?linkid=111066).

# DirectAccess

DirectAccess is a new technology introduced in Windows 7 and Windows Server 2008 R2 that provides mobile computer users working remotely with the same experience as they would have when working in the office. With DirectAccess, remote users can access corporate resources such as file shares, mail servers, intranet Web sites, or internal applications without first having to go through the steps of connecting to a virtual private network (VPN). DirectAccess automatically, and without any user intervention, establishes a bi-directional connection from client computers to the corporate network, authenticating the computer. Even before the user logs on, the computer is fully accessible to IT, allowing security and configuration management as if the computer was connected directly to the corporate network. You can further improve connection security by requiring user authentication with smart cards.

DirectAccess achieves this by establishing authenticated and encrypted IPsec tunnels for traffic sent to a DirectAccess server. The DirectAccess server acts as a gateway to the corporate network. DirectAccess is IPv6 based. If the network to which the client is connected uses IPv4, or any of the resources being accessed are IPv4-based, then IPv6-transition technologies such as 6to4, Teredo, or IP-HTTPS are used to encapsulate the IPv6 network traffic in IPv4 packets to reach the DirectAccess server.

DirectAccess seamlessly integrates with Server and Domain Isolation and Network Access Protection deployments, providing a comprehensive security, access, and health requirement solution.

For more information, see [DirectAccess](http://go.microsoft.com/fwlink/?linkid=142598) (http://go.microsoft.com/fwlink/?linkid=142598) in the Technical Library, or [DirectAccess](http://go.microsoft.com/fwlink/?linkid=147551) (http://go.microsoft.com/fwlink/?linkid=147551) on TechNet.

# Managing Windows Firewall with Advanced Security

Windows Firewall with Advanced Security provides a number of ways to implement settings on both local and remote computers. You can configure Windows Firewall with Advanced Security in the following ways:

 Configure a local or remote computer by using either the Windows Firewall with Advanced Security MMC snap-in or the netsh advfirewall command

 Deploy Windows Firewall with Advanced Security settings using Group Policy by using the Windows Firewall with Advanced Security MMC snap-in through the Group Policy Management Console or by using the netsh advfirewall command

In this section:

 [Order of Windows Firewall with Advanced Security Rules Evaluation](#zf12076833d4e438291ac36b1dde432cb)

 [Managing a Single Computer with the Snap-in](#z98e5cbb9bfe24ad98f8463b59267f67d)

 [Using the Netsh Advfirewall Command-Line Tool](#z2720bd0549594b86b933d96066525450)

 [Managing Windows Firewall with Advanced Security by Using Group Policy](#z49abd21d52bb48488e455eeabea8bede)

 [Monitoring Windows Firewall with Advanced Security](#ze8b63d25e9f641df824466965b220f75)

# Order of Windows Firewall with Advanced Security Rules Evaluation

Windows Firewall with Advanced Security supports the following types of rules:

 Windows Service Hardening. This type of built-in rule restricts services from establishing connections in ways other than they were designed. Service restrictions are configured so that Windows services can communicate only in specified ways (for example, allowed traffic might be restricted to a specified port).

 Connection security rules. This type of rule defines how and when computers authenticate using IPsec. A connection security rule can also require encryption, which helps to keep data private. Connection security rules are typically used to establish server and domain isolation, as well as to enforce NAP policy.

 Authenticated bypass rules. This type of rule allows the connection of specified computers or users even when inbound firewall rules would block the traffic. This rule requires that the network traffic from the authorized computers is authenticated by IPsec so identity can be confirmed. For example, you can allow remote firewall administration from only certain computers by creating authenticated bypass rules for those computers, or enable support for remote assistance by the Help Desk. This kind of rule is sometimes used in enterprise environments to permit “trusted” network traffic analyzers to access computers to assist in troubleshooting connectivity problems. A bypass rules lists the computers that are permitted to bypass rules that would otherwise block network traffic. Because the computer running the network analysis authenticates and is identified as being on the “allowed” list in the bypass rule, authenticated traffic from that computer is permitted through the firewall.

 Block rules. This type of rule explicitly blocks a particular type of incoming or outgoing traffic. Because these rules are evaluated before allow rules, they take precedence. Network traffic that matches both an active block and an active allow rule is blocked.

 Allow rules. This type of rule explicitly allows a particular type of incoming or outgoing traffic.

 Default rules. These rules define the action that takes place when a connection does not match any other rule. The inbound default is to block connections and the outbound default is to allow connections. The defaults can be changed in Windows Firewall Properties on a per-profile basis.

Figure 2 shows the order in which Windows Firewall with Advanced Security applies the various types of rules. This ordering of rules is always enforced, even when rules are coming from Group Policy. Rules, including those from Group Policy, are sorted and then applied. Windows Service Hardening rules are not configurable via Group Policy. Domain administrators can allow or deny local administrators the permission to create new rules.

Figure 2. Order of rules evaluation



# Managing a Single Computer with the Snap-in

Start Windows Firewall with Advanced Security

 [By using the Windows interface](#z1)

 [By using the command line](#z2)

To start Windows Firewall with Advanced Security using the Windows Server 2008 interface

|  |
| --- |
| 1. Click Start, and then select Administrative Tools.2. In Administrative Tools, click Windows Firewall with Advanced Security. |

To start Windows Firewall with Advanced Security using the Windows 7 interface

|  |
| --- |
| 1. Click Start, and then click Control Panel.2. Click System and Security.3. Click Windows Firewall.4. Click Advanced Settings. |

To start Windows Firewall with Advanced Security using the command line

|  |
| --- |
|  At a command prompt, type wf.msc. |

Figure 3 shows the Windows Firewall with Advanced Security window as it appears on Windows 7. The overview pane provides a snapshot of how Windows Firewall with Advanced Security is configured for each profile—Domain, Private, and Public. The console tree to the left provides quick access for viewing and creating inbound and outbound firewall rules and computer connection rules, and for monitoring the currently active and enforced rules. The Actions pane to the right provides a list of context-sensitive actions that change depending on what you are viewing.

Figure 3. Windows Firewall with Advanced Security Snap-in



In this section:

 [Configuring Firewall Properties](#zdf1b3cf40305474f880f03168eceb704)

 [Viewing Rules](#z711359f7c25e4de5808af903007bc068)

 [Creating New Rules](#z7135d4ebd3d746a6a0ee926428b23bb7)

 [Creating Connection Security Rules](#z3d79c776d9bb4b18bbae8711cf20c5a2)

# Configuring Firewall Properties

To configure system-wide firewall and IPsec properties, in the Overview pane, click Windows Firewall Properties. The Windows Firewall with Advanced Security on Local Computer property dialog box displays a tab for each of the three available profiles (Domain, Private, and Public) and a tab for configuring the default IPsec settings.

In this section:

 [Configuring a Profile](#z4d5eb00fdaec41a6966e8585a12e8530)

 [Configuring IPsec Settings](#zdd6a9859aaea40d7b50ac68e31bc2c86)

# Configuring a Profile

The tabs for each profile contain identical options (shown in Figure 4) that control how Windows Firewall with Advanced Security operates when the computer is connected to that type of network. Note that when Group Policy is used to configure some settings, the user is notified by the message at the top of the dialog box, and the affected controls are disabled.

Figure 4. Configuring a profile



The following are the options that you can configure for each of the three profiles:

 Firewall State. You can turn Windows Firewall with Advanced Security on or off independently for each profile.

 Inbound Connections. You can configure inbound connections to one of the following settings:

 Block (default). Windows Firewall with Advanced Security blocks inbound connections that do not match any active firewall rules. When this setting is chosen, you must create inbound allow rules to permit traffic needed by your applications.

 Block all connections. Windows Firewall with Advanced Security ignores all inbound rules, effectively blocking all inbound connections.

 Allow. Windows Firewall with Advanced Security allows inbound connections that do not match an active firewall rule. When this setting is chosen, you must create inbound block rules to prevent traffic that you do not want.

 Outbound Connections. You can configure outbound connections to one of the following settings:

 Allow (default). Windows Firewall with Advanced Security allows outbound connections that do not match any active firewall rules. When this setting is chosen, you must create outbound rules to prevent outgoing network traffic that you do not want.

 Block. Windows Firewall with Advanced Security blocks outbound connections that do not match an active firewall rule. When this setting is chosen, you must create outbound rules to allow outgoing network traffic needed by your applications.

 Protected network connections. You can configure which of the active network connections are subject to the requirements of this profile. By default, all network connections are subject to all profiles. Click Customize, and then select the network connections that you want protected.



If you clear the checkbox for a connection under one of the profiles, and the network type for that profile is detected for the connection, then the connection gets no firewall rule protection.

 Settings. Click Customize in the Settings area to configure the following settings:

 Display notifications to the user when a program is blocked from receiving inbound communications. This setting controls whether Windows displays a notification letting a user know that an inbound connection has been blocked.

 Allow unicast response to multicast or broadcast requests. This setting allows the computer to receive unicast responses to its outgoing multicast or broadcast requests.

 Apply local firewall rules. Select this option when, in addition to firewall rules applied by Group Policy that are specific to this computer, you want to allow local administrators to be able to create and apply firewall rules on this computer. When you clear this option, administrators can still create rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

 Allow local connection security rules. Select this option when, in addition to connection security rules applied by Group Policy that are specific to this computer, you want to allow local administrators to be able to create and apply connection security rules on this computer. When you clear this option, administrators can still create rules, but the rules will not be applied.

 Logging. Click Customize in the Logging area to configure the following logging options:

 Name. By default, the file is stored in %windir%\system32\logfiles\firewall\pfirewall.log.

 Size limit. By default, the size limit is 4096 kilobytes (KB).

 Log dropped packets. By default, dropped packets are not logged.

 Log successful connections. By default, successful connections are not logged.

# Configuring IPsec Settings

The IPsec Settings dialog box shown in Figure 5 is displayed when you click the Customize button on the IPsec Settings tab of the Windows Firewall with Advanced Security on Local Computer property sheet. These settings are used when you create computer connection security rules. Note that if you configure these IPsec defaults by using Group Policy, then the user is informed by the message at the top of the dialog box, and the affected controls are disabled. You can still click the Customize buttons to see the different settings, but most of the controls on those dialog boxes are also disabled.

Note

The Customize IPsec settings dialog box only allows you to create one main mode configuration. In Windows 7 and Windows Server 2008 R2, you can create additional main mode rules that enable you to use different main mode settings for connections to different computers. Previous versions of Windows Firewall with Advanced Security supported only the single main mode configuration that you can set on this dialog box. Main mode rules can be created by using the Netsh command-line tool. If a connection does not match a main mode rule, then the main mode settings on this dialog box are used for the connection. For more information, see [Netsh AdvFirewall MainMode Commands](http://go.microsoft.com/fwlink/?linkid=147508) (http://go.microsoft.com/fwlink/?linkid=147508)

Figure 5. Configuring IPsec settings



This dialog box allows you to choose the following options:

 Key Exchange (Main Mode). To enable secure communication, two computers must be able to access the same shared key without transferring that key across the network. Click the Customize button to configure security methods, key exchange algorithms, and key lifetimes. These settings are used to protect the IPsec negotiations that in turn determine the protection used for the rest of the data sent over the connection.

 Data Protection (Quick Mode). IPsec data protection defines the algorithms and protocols used to provide data integrity and encryption for a connection. Data integrity ensures that data is not modified during transit. Data encryption uses cryptography to conceal the information. Windows Firewall with Advanced Security uses Authentication Header (AH) or Encapsulating Security Payload (ESP) to provide data protection. Windows Firewall with Advanced Security uses ESP for data encryption.

 Authentication Method. This setting lets you choose the default authentication method for IPsec connections on the local computer, unless a different method is specified by a rule or by Group Policy settings. The default authentication method is Kerberos version 5, which is useful on rules that implement domain isolation. You can also restrict connections to only those computers that have a certificate from a specified certification authority (CA).

# Viewing Rules

Rules allow specified programs, protocols, or services to pass through the firewall. For example, when you enable Remote Desktop in Windows 7 or Windows Vista, Windows creates a rule to allow inbound Remote Desktop connection attempts to reach the computer. To view current rules in Windows Firewall with Advanced Security, in the console tree, click either the Inbound Rules folder or the Outbound Rules folder. Figure 6 shows an example of the Inbound Rules folder. The Inbound Rules folder shows all of the rules currently defined on the computer. To see only the rules that are currently active and enforced, click the Inbound Rules node under Monitoring instead.

Figure 6. Viewing inbound rules



To enable a rule, click the rule, and in the Actions list, click Enable Rule. To disable a rule, click the rule, and then click Disable Rule.

Note

If Group Policy has configured Windows Firewall with Advanced Security settings on your computer, then you might not be able to enable or disable firewall or connection security rules. If this is the case, then the Enable Rule and Disable Rule options in the Actions list do not appear.

To view and modify the properties for a rule, click the rule and then click Properties. The property sheet for a rule (shown in Figure 7) displays the tabs and options listed in Table 1.

Figure 7. Viewing properties for a rule



Table 1. Properties for a rule that can be configured

|  |  |  |
| --- | --- | --- |
| Tab | Option | Use |
| General | Name | Type a name for the rule. |
| Description | Type a description for the rule. |
| Enabled | Turn the rule on or off. This setting indicates whether the rule is active. Disabled rules do not affect traffic that is allowed or blocked. |
| Action | Configure the following options: Allow the connection. Use to allow any connection that matches all criteria specified by the rule. This option does not check whether the traffic is protected by IPsec. Allow the connection if it is secure. Use to allow any connection that is protected by IPsec and that matches all criteria specified in the rule. You can further specify that the connection must also be encrypted in order to be allowed. You must separately create a connection security rule that specifies how traffic is protected; otherwise, the traffic will never match this rule.Note In Windows Vista and Windows Server 2008, this option was called Allow only secure connections.  Block the connection. Use to create a rule that blocks connections that meet the criteria specified in the rule. |
| Programs and Services | Programs | Specify the full path to the executable file on the local computer. |
| Services | Specify the short name of the service to which the rule applies. This is mapped to the security identifier (SID) associated with the service. |
| Computers | Authorized computers | Specify that connections related to this rule are allowed only from a group of computers that you create. You can select this option only if you have also selected the option Allow the connection if it is secure and if the connection has been protected using a credential that provides the Active Directory identity information (most commonly, computer Kerberos v5). |
| Exceptions | Specify computers that are not permitted to match this rule, even if they are a member of a computer group that is in the Authorized computers list. This simplifies rule creation by supporting “all computers except this one” type of rules. |
| Users | Authorized users | Specify that connections related to this rule are allowed only from a group of users that you create. You can select this option only if you have also selected the option Allow only secure connections and if the connection has been protected using a credential that provides the Active Directory identity information (most commonly, computer Kerberos v5). |
| Exceptions | Specify users that are not permitted to match this rule, even if they are a member of a user group that is in the Authorized users list. This simplifies rule creation by supporting “all users except this one” type of rules. |
| Protocols and Ports | Protocol Type | Specify any type of IP protocol (for example, TCP or UDP). |
| Protocol Number | Windows automatically specifies a port number based on the protocol type. If you are using a custom protocol type, you can specify a protocol number. |
| Local port | Specify the local port over which traffic can pass. In Windows 7 and Windows Server 2008 R2 you can specify a port range, such as 5000-5010. You can also specify one of the following keywords:  RPC Dynamic Ports RPC Endpoint Mapper IPHTTPS Edge Traversal |
| Remote port | Specify the remote port over which traffic can pass. In Windows 7 and Windows Server 2008 R2 you can specify a port range, such as 5000-5010. |
| Internet Control Message Protocol (ICMP) Settings | Specify ICMP types and codes. This option is available only if the protocol type is ICMPv4 or ICMPv6. |
| Scope | Local IP address and Remote IP address | Specify the local and remote IPv4 or IPv6 addresses, ranges of addresses, and subnets to which the rule applies. |
| Advanced | Profiles | Specify the profiles to which the rule applies. This can be any combination of domain, public, and private profiles. |
| Interface types | Specify which interface type a computer connection security rule is applied to, such a local area network, wireless network adapter, or other connection type. |
| Edge traversal | Specify whether unsolicited inbound packets that have passed through an edge device such as a NAT router are permitted |

# Creating New Rules

Windows Firewall with Advanced Security allows you to create the following types of firewall rules:

 [Program rule](#z3). This type of rule allows traffic for a specified program. You can identify the program by program path and executable file name.

 [Port rule](#z4). This type of rule allows traffic on a specified TCP or UDP port number or range or port numbers.

 Predefined rule. Windows includes a number of Windows functions that you can enable, such as File and Printer Sharing, Remote Assistance, and Windows Collaboration. Creating a predefined rule actually creates a group of rules that enable the specified Windows functionality to access the network.

 Custom rule. This type of rule allows you to create a rule that you might not be able to create using the other types of rules. A custom rule allows you to combine any of the rule elements together.

To create a program rule on a local computer

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security console tree, select and then right-click Inbound Rules or Outbound Rules, depending on the type you want to create, and click New Rule.This action opens either the New Inbound Rule Wizard or the New Outbound Rule Wizard. The steps for creating an inbound or outbound rule are identical.2. On the Rule Type page, click Program, and then click Next.3. On the Program page, click This program path. Type the path for the executable file for the program, or click Browse to find the program by using Windows Explorer. Click Next.4. On the Action page (shown in Figure 8), select the desired behavior, and then click Next.Figure 8. Specifying actions for a rule5. If you selected Allow the connection if it is secure on the Action page, then the Users and Computers pages are displayed, where you can specify user and computer accounts that are permitted to access the computer through this firewall rule. If you specify users or computers then you must separately create a connection security rule that requires network traffic that matches this rule to be authenticated.6. On the Profile page, select the profiles to which the rule should apply, and then click Next.7. On the Name page, type a name and a description for the rule, and then click Finish. |

To create a port rule on a local computer

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security console tree, select and then right-click Inbound Rules or Outbound Rules, depending on the type you want to create, and click New Rule.This action opens either the New Inbound Rule Wizard or the New Outbound Rule Wizard. The steps for creating an inbound or outbound rule are identical.2. On the Rule Type page, click Port, and then click Next.3. On the Protocol and Ports page (shown in Figure 9), select whether the rule should use the TCP or UDP protocol. Click Specific Local Ports, type in the numbers of the ports for which you need to create the rule, and then click Next.Note For an outbound rule, it is Specific Remote Ports.Figure 9. Selecting a port number for a port rule4. On the Action page, select the desired behavior, and then click Next.5. If you selected Allow the connection if it is secure on the Action page, then the Users and Computers pages are displayed, where you can specify user and computer accounts that are permitted to access the computer through this firewall rule. If you specify users or computers then you must separately create a connection security rule that requires network traffic that matches this rule to be authenticated.6. On the Profile page, select the profiles to which the rule should apply, and then click Next.7. On the Name page, type a name and a description for the rule, and then click Finish. |

# Creating Connection Security Rules

A connection security rule forces two peer computers to authenticate before they can establish a connection and to secure information transmitted between the two computers. Windows Firewall with Advanced Security uses IPsec to enforce these rules.

To create a connection security rule

|  |
| --- |
| 1. In Windows Firewall with Advanced Security, in the console tree, click Connection Security Rules.2. In the Actions list, click New Rule.The Rule Type page, shown in Figure 10, allows you to select the type of rule you want to create. Select a type, and use the wizard to configure the new rule according to the information in the following sections.Figure 10. Using the New Authentication Rule Wizard to create a rule |

By using Windows Firewall with Advanced Security, you can create the rule types described in the following sections.

## Isolation

An isolation rule isolates computers by restricting inbound connections based on credentials, such as domain membership or compliance with policies that define the required software and system configurations. Isolation rules allow you to implement a server or domain isolation strategy. When you create an isolation rule, you will see the following wizard pages:

 Requirements. You can choose when authentication is required:

 Request authentication for inbound and outbound connections

 Require authentication for inbound connections and request authentication for outbound connections

 Require authentication for inbound and outbound connections

 Authentication Method. You can select from the following authentication methods:

 Default. This selection uses the current computer default selections specified on the IPsec Settings tab of the Windows Firewall Properties page.

 Computer and user (Kerberos V5). This method uses both computer- and user-based Kerberos V5 authentication to restrict connections to domain-joined users and computers. User authentication, and therefore this method, is compatible only with computers running Windows Vista and later.

 Computer (Kerberos V5). This method uses Kerberos V5 authentication to restrict connections to domain-joined computers. This method is compatible with computers running Windows 2000 or later.

 Advanced. This setting allows you to designate multiple authentication methods, such as computer certificate, NTLMv2, and preshared key.

 Profile. Choose the profiles (Domain, Public, and Private) to which the rule applies.

 Name. Name the rule and type an optional description.

## Authentication exemption

You can use an authentication exemption to designate computers that do not require authentication. Computers in an isolated domain can communicate with computers listed in this rule even though they cannot authenticate. You can designate computers by IP address, an IP address range, a subnet, or a predefined group, such as gateway. When you create an authentication exemption rule, you must configure options on the following wizard pages:

 Exempt Computers. Add computers that are exempt from authentication. You can add a computer by IP address or IP address range, or you can add a computer based on its role, such as the default gateway, or the DNS servers that the local computer is configured to use.

 Profile. Choose the profiles (Domain, Public, and Private) to which the rule applies.

 Name. Name the rule and type an optional description.

## Server-to-server

A server-to-server rule protects connections between specified computers. This type of rule usually protects connections between servers. When you create the rule, you specify the network endpoints between which communications are protected. You then designate authentication requirements and the types of authentication that you want to use. When you create a server-to-server rule, you must configure options on the following wizard pages:

 Endpoints. Specify the computers that are part of Endpoint 1 and Endpoint 2. Endpoint 1 can contain all computers, computers specified by IP address, or computers that are accessible through a specified connection type (such as a local area network or wireless connection). Endpoint 2 can contain all computers or computers specified by IP address.

 Requirements. Choose when authentication is required. Options are identical to those described in the section “Isolation.”

 Authentication Method. Choose a method for authentication, including Computer Certificate or a customized Advanced method.

 Profile. Choose the profiles (Domain, Public, and Private) to which the rule applies.

 Name. Name the rule and type an optional description.

## Tunnel

A tunnel rule allows you to protect connections between gateway computers and is typically used when connecting across the Internet between two security gateways. You must specify the tunnel endpoints by IP address and specify the authentication method by configuring the following wizard pages:

 Tunnel Type. Specify the type of tunnel that you want to create: client-to-gateway, or gateway-to-client, or a custom-defined tunnel. You can also specify whether traffic that arrives at a tunnel endpoint that is already IPsec-protected must be encapsulated a second time by the tunnel rule before being forwarded to the other tunnel endpoint.

 Requirements. Specify whether network traffic passing through the tunnel must be authenticated, and if so, whether authentication is requested or required.

 Tunnel Endpoints. Identify by IP address or IP address range the computers that serve as gateways to computers that are part of each endpoint – Endpoint 1 and Endpoint 2. Also identify by IP address which tunnel computer in each endpoint is closest to computers in that endpoint. The options available on this page depend on the tunnel type you selected on the first page.

 Authentication Method. Choose a method for authentication, including Computer Certificate, or a customized Advanced method.

 Profile. Choose the profiles (Domain, Public, and Private) to which the rule applies.

 Name. Name the rule and type an optional description.

## Custom

Use a custom rule to authenticate connections between two endpoints when you cannot set up authentication rules you need by using the other types of rules available in the new Connection Security Rule wizard. You can configure options on the following wizard pages:

 Endpoints. Specify the computers that are part of Endpoint 1 and Endpoint 2. Endpoint 1 can contain all computers, computers specified by IP address, or computers that are accessible through a specified connection type (such as a local area network or wireless connection). Endpoint 2 can contain all computers or computers specified by IP address.

 Requirements. Choose when authentication is required. Options are identical to those described in the section “Isolation.”

 Authentication Method. Choose the authentication method. Options are identical to those described in the section “Isolation.”

 Protocol and Ports. Specify the protocol, and if TCP or UDP, the source and destination ports that are affected by this connection security rule.

 Profile. Choose the profiles (Domain, Public, and Private) to which the rule applies.

 Name. Name the rule and type an optional description.

# Using the Netsh Advfirewall Command-Line Tool

Netsh is a command-line tool that you can use to configure settings for network components. You can configure Windows Firewall with Advanced Security settings through commands in the netsh advfirewall context. Using Netsh, you can create scripts to automatically configure Windows Firewall with Advanced Security settings, create firewall rules and connection security rules, monitor active connections, and display the configuration and status of Windows Firewall with Advanced Security.

To enter the netsh context, at an elevated command prompt, type:

netsh

When you enter the netsh context, the command prompt will display the netsh> prompt. From there, enter the advfirewall context by typing:

advfirewall

After you are in the advfirewall context, you can type commands in that context. Commands include the following:

 export. Exports the current firewall policy to a file.

 dump. This command is not implemented in the advfirewall context. No output is produced, and no error messages are generated.

 help. Displays a list of available commands.

 import. Imports a firewall policy from the specified file.

 reset. Restores Windows Firewall with Advanced Security to the default configuration.

 set. Supports the following commands:

 set file. Copies the console output to a file.

 set machine. Sets the current computer on which to operate.

 show. Shows the properties for a particular profile. For example:

 show allprofiles

 show domainprofile

 show privateprofile

 show publicprofile

In addition to the commands available for the advfirewall context, advfirewall also supports subcontexts. To enter a subcontext, type the name of the subcontext at the netsh advfirewall> prompt. The available subcontexts are:

 consec. Allows you to view and configure computer security connection rules.

 firewall. Allows you to view and configure firewall rules.

 mainmode. Allows you to view and configure main mode configuration rules.

 monitor. Allows you to view the current IPsec, firewall, and main mode states, and the current quick mode and main mode security associations established on the local computer. You can also monitor other aspects of IPsec by using the netsh wfp context.

Note

In any netsh context, you can type help to view a full list of commands, including commands specific to a context. For information and syntax about using a command, type <commandname> /?.

For more information about netsh, see [Netsh Technical Reference](http://go.microsoft.com/fwlink/?LinkId=178668) (http://go.microsoft.com/fwlink/?LinkId=178668), and [Netsh Commands for Windows Firewall with Advanced Security](http://go.microsoft.com/fwlink/?LinkId=178669) (http://go.microsoft.com/fwlink/?LinkId=178669).

# Managing Windows Firewall with Advanced Security by Using Group Policy

To centralize the configuration of large numbers of computers in an organizational network that uses the Active Directory Domain Services (AD DS), you can deploy settings for Windows Firewall with Advanced Security through Group Policy. Group Policy provides access to the full feature set of Windows Firewall with Advanced Security, including profile settings, rules, and computer connection security rules. In fact, you configure Group Policy settings for Windows Firewall with Advanced Security by opening the same snap-in through the Group Policy Management Console. You can also configure Group Policy settings with the netsh advfirewall context by using the set store command to point netsh to a Group Policy object instead of the local computer. Because the domain-member computer requests Group Policy updates, the traffic is therefore solicited and is not dropped by default when Windows Firewall with Advanced Security is enabled (unless the outbound default is configured to block traffic).

Note

When you use Group Policy to configure Windows Firewall with Advanced Security in an organizational network, Group Policy might disable some local Windows Firewall with Advanced Security configuration options, even for local administrators.

In Windows Vista and later versions of Windows, the Network Location Awareness feature provides the flexibility to ensure that Group Policy is correctly applied in different situations. In earlier versions of the Windows operating system, Windows processes Group Policy under the following circumstances:

 Computer policies are processed when the Windows operating system starts.

 User policies are processed when a user logs on.

 Both computer and user policies are refreshed periodically.

In addition to these circumstances, Windows Vista and later versions of Windows also process Group Policy under the following circumstances:

 Computer and user policies are processed when a computer establishes a virtual private network (VPN) connection with a remote site.

 Computer and user policies are processed when a computer comes out of hibernation or standby mode.

The additional processing helps to ensure that computers obtain the most recent Group Policy settings more frequently and whenever the computer changes connections.

For more information about using Group Policy to deploy Windows Firewall with Advanced Security settings and rules, see [Step-by-Step Guide to Deploying Policies for Windows Firewall with Advanced Security](http://go.microsoft.com/fwlink/?linkid=96318) (http://go.microsoft.com/fwlink/?linkid=96318).

# Monitoring Windows Firewall with Advanced Security

Windows Firewall with Advanced Security includes built-in tools for monitoring the currently active firewall rules, connection security rules, and security associations (SAs). Expand Monitoring to monitor the Firewall, Connection Security Rules, and Security Associations.

## Firewall

Click Firewall to monitor all active enabled rules, including rules for the active profile and rules distributed by using Group Policy.

## Connection Security Rules

Click Connection Security Rules to monitor all of the enabled connection security rules with detailed information about their settings.

## Security Associations

Expand Security Associations to monitor all of the Main Mode and Quick Mode SAs currently established on the local computer, with detailed information about their settings and endpoints. An SA defines the shared security information used to protect the communications between two computers.

 Main Mode

Click Main Mode to see all of the Main Mode SAs with detailed information about their settings and endpoints. You can use this folder to view the IP addresses of the endpoints.

 Quick Mode

Click Quick Mode to see all of the Quick Mode SAs with detailed information about their settings and endpoints. You can use this folder to view the IP addresses of the endpoints.

# Additional Resources

For more information about the features and technologies discussed in this document, see the following resources:

 [Windows Firewall with Advanced Security and IPsec](http://go.microsoft.com/fwlink/?linkid=96525) in the Windows Server Technical Library (http://go.microsoft.com/fwlink/?linkid=96525).

 [Windows Firewall](http://go.microsoft.com/fwlink/?linkid=95393) on TechNet (http://go.microsoft.com/fwlink/?linkid=95393).

 [Server and Domain Isolation](http://go.microsoft.com/fwlink/?linkid=95395) on TechNet (http://go.microsoft.com/fwlink/?linkid=95395).

 [IPsec](http://go.microsoft.com/fwlink/?linkid=95394) on TechNet (http://go.microsoft.com/fwlink/?linkid=95394).