

Step-by-Step Guide: Deploying Windows Firewall and IPsec Policies

Microsoft Corporation

Updated: November 2009

Author: Dave Bishop

Editor: Scott Somohano

Abstract

This guide shows you how to centrally configure and distribute commonly used settings and rules for Windows Firewall with Advanced Security by describing typical tasks in a common scenario. you get hands-on experience in a lab environment using Group Policy management tools to create and edit GPOs to implement typical firewall settings. You also configure GPOs to implement common server and domain isolation scenarios and see the effects of those settings. This guide applies to computers running Windows® 7, Windows Vista®, Windows Server® 2008 R2, and Windows Server® 2008.



The information 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 Step-by-Step Guide 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, and Windows XP are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Step-by-Step Guide: Deploying Windows Firewall and IPsec Policies 5](#_Toc245784883)

[Scenario Overview 6](#_Toc245784884)

[Technology Review for Deploying Windows Firewall with Advanced Security 9](#_Toc245784885)

[Network Location Awareness 9](#_Toc245784886)

[Host Firewall 11](#_Toc245784887)

[Connection Security and IPsec 13](#_Toc245784888)

[Group Policy 16](#_Toc245784889)

[Requirements for Performing the Scenarios 17](#_Toc245784890)

[Examining Default Settings on Clients and Servers 21](#_Toc245784891)

[Step 1: Starting Windows Firewall in Control Panel 22](#_Toc245784892)

[Step 2: Examining the Basic Options Available by Using the Control Panel Interface 24](#_Toc245784893)

[Step 3: Examining the Basic Options by Using the Netsh Command-Line Tool 26](#_Toc245784894)

[Step 4: Examining the Basic Options Available When Using the Windows Firewall with Advanced Security MMC snap-in 27](#_Toc245784895)

[Step 5: Examine the Differences in Functionality Between the MMC Snap-in and the Netsh Command-line Tool 29](#_Toc245784896)

[Deploying Basic Settings by Using Group Policy 32](#_Toc245784897)

[Step 1: Creating OUs and Placing Computer Accounts in Them 32](#_Toc245784898)

[Step 2: Creating the GPOs to Store Settings 34](#_Toc245784899)

[Step 3: Adding the GPO Setting to Enable the Firewall on Member Client Computers 34](#_Toc245784900)

[Step 4: Deploying the Initial GPO with Test Firewall Settings 36](#_Toc245784901)

[Step 5: Adding the Setting that Prevents Local Administrators from Applying Conflicting Rules 37](#_Toc245784902)

[Step 6: Configuring the Rest of Your Client Computer Firewall Settings 39](#_Toc245784903)

[Step 7: Creating WMI and Group Filters 41](#_Toc245784904)

[Step 8: Enabling Firewall Logging 45](#_Toc245784905)

[Creating Rules that Allow Required Inbound Network Traffic 49](#_Toc245784906)

[Step 1: Configuring Predefined Rules by Using Group Policy 50](#_Toc245784907)

[Step 2: Allowing Unsolicited Inbound Network Traffic for a Specific Program 52](#_Toc245784908)

[Step 3: Allowing Inbound Traffic to a Specified TCP or UDP Port 55](#_Toc245784909)

[Step 4: Allowing Inbound Network Traffic that Uses Dynamic RPC 56](#_Toc245784910)

[Step 5: Viewing the Firewall Log 61](#_Toc245784911)

[Creating Rules that Block Unwanted Outbound Network Traffic 62](#_Toc245784912)

[Step 1: Configuring the Default Outbound Firewall Behavior to Block 62](#_Toc245784913)

[Step 2: Allowing Network Traffic for a Program by Using an Outbound Rule 65](#_Toc245784914)

[Deploying a Basic Domain Isolation Policy 66](#_Toc245784915)

[Step 1: Creating a Connection Security Rule that Requests Authentication 68](#_Toc245784916)

[Step 2: Deploying and Testing Your Connection Security Rules 71](#_Toc245784917)

[Step 3: Changing the Isolation Rule to Require Authentication 73](#_Toc245784918)

[Step 4: Testing Isolation with a Computer That Does Not Have the Domain Isolation Rule 74](#_Toc245784919)

[Step 5: Creating Exemption Rules for Computers that are Not Domain Members 75](#_Toc245784920)

[Isolating a Server by Requiring Encryption and Group Membership 76](#_Toc245784921)

[Step 1: Creating the Security Group 77](#_Toc245784922)

[Step 2: Modifying a Firewall Rule to Require Group Membership and Encryption 78](#_Toc245784923)

[Step 3: Creating a Firewall Rule for the Client to Support Encryption 79](#_Toc245784924)

[Step 4: Testing the Rule When Admin1 Is Not a Member of the Group 80](#_Toc245784925)

[Step 5: Adding Admin1 to the Group and Testing Again 81](#_Toc245784926)

[Creating Firewall Rules that Allow IPsec-protected Network Traffic (Authenticated Bypass) 82](#_Toc245784927)

[Step 1: Adding and Testing a Firewall Rule that Blocks Standard Telnet Traffic 83](#_Toc245784928)

[Step 2: Modifying a Telnet Firewall Allow Rule to Override Block Rules 84](#_Toc245784929)

[Creating Tunnel Mode IPsec Rules 85](#_Toc245784930)

[Step 1: Reconfigure your Lab Computers to Support the IPsec Client-to-Gateway Scenario 86](#_Toc245784931)

[Step 2: Create the Connection Security Rules for the Remote Client and IPsec Gateway 89](#_Toc245784932)

[Step 3: Test Your Tunnel Mode Rules 91](#_Toc245784933)

[Summary 92](#_Toc245784934)

[Additional References 92](#_Toc245784935)

Step-by-Step Guide: Deploying Windows Firewall and IPsec Policies

This step-by-step guide illustrates how to deploy Active Directory® Group Policy objects (GPOs) to configure Windows Firewall with Advanced Security on computers that are running Windows® 7, Windows Vista®, Windows Server® 2008 R2, and Windows Server® 2008. Although you can configure a single server locally by using Group Policy Management and other tools directly on the server, that method is not efficient and does not guarantee consistency when you have many computers to configure. When you have multiple computers to manage, you can instead create and edit GPOs, and then apply those GPOs to the computers in your organization.

The goal of a Windows Firewall with Advanced Security configuration in your organization is to improve the security of each computer by blocking unwanted network traffic from entering the computer and protecting wanted network traffic as it traverses the network. Network traffic that does not match the rule set configured in Windows Firewall with Advanced Security is dropped. You can also require that the network traffic which is allowed must be protected by using authentication or encryption. The ability to manage Windows Firewall with Advanced Security by using Group Policy lets an administrator apply consistent settings across the organization in a way that is not easily circumvented by the user.

In this guide, you get hands-on experience in a lab environment that uses Group Policy management tools to create and edit GPOs to implement typical firewall and connection security settings and rules. You configure GPOs to implement common server and domain isolation scenarios and see the effects of those settings.

Your feedback is valuable and welcome! Please send your comments and suggestions to [Windows Firewall with Advanced Security Documentation Feedback](mailto://wfasdoc@microsoft.com?subject=Feedback%20on%20IPsec%20and%20Firewall%20Documentation%20–%20WFAS%20SxS%20Deploying%20FW%20and%20IPsec%20Policies%20Guide&body=I%20want%20to%20provide%20the%20following%20feedback%20on%20the%20document%20Step-by-Step%20Guide:%20Deploying%20Windows%20Firewall%20and%20IPsec%20Policies.%0A%0A) (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:

 [Scenario Overview](#z08a840b63777488b975ddf7d7b51ce39)

 [Technology Review for Deploying Windows Firewall with Advanced Security](#z40f2679a17a5450986b7492db5cd4b30)

 [Requirements for Performing the Scenarios](#ze245fa7756ea4c13bb2d83ce018e5834)

 [Examining Default Settings on Clients and Servers](#zb872d80528684fe5b0af5abc5549729a)

 [Deploying Basic Settings by Using Group Policy](#z814a075710a14b38a141b76332482e1c)

 [Creating Rules that Allow Required Inbound Network Traffic](#ze5c2f8ea3b1d44df8307ea5bfa96b7e0)

 [Creating Rules that Block Unwanted Outbound Network Traffic](#zc0b58af6447e4a47ae46bb68fdeaf203)

 [Deploying a Basic Domain Isolation Policy](#z626058b754b44fc9bbdf7a427bedf467)

 [Isolating a Server by Requiring Encryption and Group Membership](#zfb995b0bce8b4507a6531acdf5ef8ff5)

 [Creating Firewall Rules that Allow IPsec-protected Network Traffic (Authenticated Bypass)](#zd9891d8917d74cf3a08de4a46904a7a2)

 [Creating Tunnel Mode IPsec Rules](#ze8e462c96d324ce89d07080a9f7f2b19)

 [Summary](#z917f57d811774da4aa754e08d94f5876)

 [Additional References](#ze4248de52d0747219c54163e351e33fb)

Next topic: [Scenario Overview](#z08a840b63777488b975ddf7d7b51ce39)

Scenario Overview

In this guide, you learn about how to create and deploy settings for Windows Firewall with Advanced Security by stepping through procedures that illustrate the common tasks you have to perform in typical scenarios.

Specifically, you configure settings in GPOs to control the following Windows Firewall with Advanced Security options:

 Enable or disable the Windows Firewall, and configure its basic behavior.

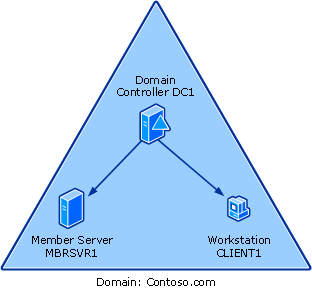
 Determine which programs and network ports are allowed to receive incoming network traffic.

 Determine which outgoing network traffic is allowed or blocked.

 Support network traffic that uses multiple or dynamic ports, such as those that use Remote Procedure Call (RPC), or the File Transfer Protocol (FTP).

 Require that all network traffic entering specific servers be protected by Internet Protocol security (IPsec) authentication and optionally encrypted.

You work with several computers that perform common roles found in a typical network environment. These include a domain controller, a member server, and a client computer, as shown in the following illustration.



The scenario described in this guide includes viewing and configuring firewall settings, and configuring a domain isolation environment. It also includes server isolation, which requires group membership to access a server and can optionally require that all traffic to the server is encrypted. Finally, it includes a mechanism to allow trusted network devices to bypass firewall rules for troubleshooting.

Each of the scenario steps are described in the following sections.

Examining default settings on clients and servers

[In this section](#zb872d80528684fe5b0af5abc5549729a), you use Windows Firewall settings in Control Panel, the netsh command-line tool, and the Windows Firewall with Advanced Security Microsoft Management Console (MMC) snap-in to examine the default Windows Firewall with Advanced Security settings on the both the CLIENT1 and MBRSVR1 computers. By using the tools directly on a local computer is useful to see the current configuration and the firewall and connection security rules that are active on the computer. This section also compares the features that can be configured by using the Windows Firewall with Advanced Security MMC and the netsh command-line tool.

Deploying basic firewall settings by using Group Policy

[This section](#z814a075710a14b38a141b76332482e1c) shows you how to create a Group Policy object (GPO) that contains basic firewall settings, and then apply that GPO to the client computer. To ensure that only the correct computers can apply the GPO settings, you use security group filtering and Windows Management Instrumentation (WMI) filtering to restrict the GPO to only those computers that are in a specified computer group and that are running the specified version of Windows.

The GPO that you configure includes some of the basic Windows Firewall with Advanced Security settings that are part of a typical enterprise's GPO settings, such as:

 Any local firewall setting created by a user, even a local administrator, is ignored.

 Ensure that the firewall is enabled with your specified handling of network traffic, and cannot be disabled.

 The computer does not display the notification when Windows Firewall with Advanced Security blocks a program from listening on a network port.

Creating rules that allow required incoming network traffic

By default, Windows Firewall blocks all incoming network connections that do not match an “allow” rule. On client computers that do not host any services, this might be sufficient. But for any program that acts as a network service, you must create rules to permit the unsolicited network packets from remote computers that want to connect to the application or network service. [In this section](#ze5c2f8ea3b1d44df8307ea5bfa96b7e0), you create and modify inbound firewall allow rules to do the following:

 Use predefined rule groups to support common network services.

 Allow a program to listen for any network traffic it needs to operate.

 Allow a program to listen for network traffic on a specified TCP or UDP port only.

 Allow a network service to listen for network traffic.

 Limit network traffic from only specified IP addresses, and to specific types of networks.

 Apply different firewall behavior based on the network location type to which the computer is connected.

 Support programs that use the dynamic port assigning capabilities of RPC.

One of the main benefits of integrating firewall and IPsec into the single Windows Firewall with Advanced Security interface is the ability to create firewall rules that allow network traffic only if the traffic is protected by IPsec. These rules are discussed in the [Server Isolation](#zfb995b0bce8b4507a6531acdf5ef8ff5) and [Authenticated Bypass](#zd9891d8917d74cf3a08de4a46904a7a2) sections of this guide.

Blocking unwanted outbound network traffic

By default, Windows Firewall allows all outbound network connections. Because of the very large number and variety of potential outbound network-aware client programs, it can be a very large amount of work to attempt to restrict outbound traffic. However, in some organizations, where the approved list of applications is known, and security dictates that no other application must be permitted to access the network, then Windows Firewall with Advanced Security supports changing the default outbound rule to block network traffic that is not permitted by an outbound allow rule. [In this section](#zc0b58af6447e4a47ae46bb68fdeaf203), you configure the firewall to block all outbound traffic, and then create outbound firewall rules that allow only approved programs to send outbound traffic from a computer.

Deploying a basic domain isolation policy

[In this section](#z626058b754b44fc9bbdf7a427bedf467), you create IPsec connection security rules on your domain member computers that allow incoming network connection requests from authenticated domain member computers only.

Isolating a server by requiring encryption and group membership

[In this section](#zfb995b0bce8b4507a6531acdf5ef8ff5), you expand on the authentication rules created in the previous section, by creating connection security and firewall rules that require that a server or group of servers allow network traffic only from computers that are members of an authorized group. The rules also specify that the traffic to and from these servers must be encrypted.

Creating firewall rules that allow IPsec-protected network traffic to bypass block rules

When you have the firewall and connections security rules up and running, you typically end up blocking network security tools, such as port scanners from being able to do their jobs. Windows Firewall with Advanced Security lets you create firewall allow rules that can override block rules only when certain requirements are met. [In this section](#zd9891d8917d74cf3a08de4a46904a7a2), you configure firewall and connection security rules to allow IPsec-protected network traffic to bypass the firewall block rules. You also further restrict the rules to allow only specifically authorized users or computers, such as the network port scanners used by network troubleshooting and security teams.

Creating tunnel mode IPsec connection security rules

The rules that you create for the previously described scenarios all use IPsec Transport mode rules. Transport mode provides end-to-end protection from the originating source host all the way to the ultimate destination host. IPsec supports another mode of operation called tunnel mode, where the IPsec traffic is protected only for part of the path between the two hosts. [In this section](#ze8e462c96d324ce89d07080a9f7f2b19), you configure tunnel mode connection security rules to allow a client computer to access a remote network through an IPsec gateway.

Next topic: [Technology Review for Deploying Windows Firewall with Advanced Security](#z40f2679a17a5450986b7492db5cd4b30)

Technology Review for Deploying Windows Firewall with Advanced Security

Windows Firewall with Advanced Security combines a host-based firewall and an Internet Engineering Task Force (IETF)-compliant implementation of Internet Protocol security (IPsec).

As a host-based firewall, Windows Firewall with Advanced Security runs on each computer that is running Windows Vista® or a later version of Windows to provide local protection from network attacks that might pass through your perimeter network firewall or originate from inside your organization.

Windows Firewall with Advanced Security also provides IPsec-based computer-to-computer connection security which lets you protect the network data by setting rules that require authentication, integrity checking, or encryption when your computers exchange data.

Windows Firewall with Advanced Security works with both Internet Protocol version 4 (IPv4) and IPv6 traffic.

This section of the guide provides a brief review of these features to support your understanding of the scenarios that you examine in later sections of this guide.

 [Network Location Awareness](#z43bea15e5d4c4b81a7e4b17c2fe53d47)

 [Host Firewall](#z4eb905238d874b79a7ef4a6a1fe4e513)

 [Connection Security and IPsec](#z7336450e2796477abc55201bb0a10d7c)

 [Group Policy](#z7863c88524e44ad79992b98b5fe843ab)

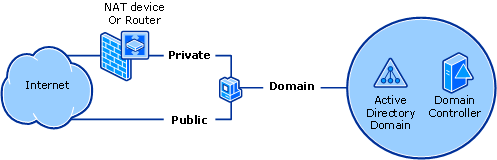
Next topic: [Network Location Awareness](#z43bea15e5d4c4b81a7e4b17c2fe53d47)

Network Location Awareness

Windows Vista® and later versions of Windows support network location awareness, which enables network-interacting programs to change their behavior based on how the computer is connected to the network. In the case of Windows Firewall with Advanced Security, you can create rules that apply only when the profile associated with a specific network location type is active on your computer.

How Network Location Awareness works

The following diagram shows the network location types that can be detected by Windows.



Computers that are running Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 detect the following network location types:

 Public. By default, the public network location type is assigned to any new networks when they are first connected. A public network is considered to be shared with the world, with no protection between the local computer and any other computer. Therefore, the firewall rules associated with the public profile are the most restrictive.

 Private. The private network location type can be manually selected by a local administrator for a connection to a network that is not directly accessible by the public. This connection can be to a home or office network that is isolated from publicly accessible networks by using a firewall device or a device that performs network address translation (NAT). Wireless networks assigned the private network location type should be protected by using an encryption protocol such as Wi-Fi Protected Access (WPA) or WPAv2. A network is never automatically assigned the private network location type; it must be assigned by the administrator. Windows remembers the network, and the next time that you connect to it, Windows automatically assigns the network the private network location type again. Because of the higher level of protection and isolation from the Internet, private profile firewall rules typically allow more network activity than the public profile rule set.

 Domain. The domain network location type is detected when the local computer is a member of an Active Directory domain, and the local computer can authenticate to a domain controller for that domain through one of its network connections. An administrator cannot manually assign this network location type. Because of the higher level of security and isolation from the Internet, domain profile firewall rules typically permit more network activity than either the private or public profile rule sets. On a computer that is running Windows 7 or Windows Server 2008 R2, if a domain controller is detected on any network adapter, then the Domain network location type is assigned to that network adapter. On computers that are running Windows Vista or Windows Server 2008, then the Domain network location type is applied only when a domain controller can be detected on the networks attached to every network adapter.

Windows Firewall with Advanced Security stores its setting and rules in profiles, and supports one profile for each network location type. The profiles associated with the currently detected network location types are the ones that are applied to the computer. If the network location type assigned to a network changes then the rules in the profile associated with the new network location type automatically apply.

When you have multiple network adapters attached to your computer, you can be attached to networks of different types. Computers that are running Windows 7 and Windows Server 2008 R2 support different network location types, and therefore profiles, for each network adapter at the same time. Each network adapter is assigned the network location appropriate for the network to which it is connected. Windows Firewall then enforces only those rules that apply to that network type’s profile. So certain types of traffic are blocked when coming from a network adapter connected to a public network, but those same types might be permitted when coming from a private or domain network.

Important

Windows Vista, Windows Server 2008, Windows XP, and Windows Server 2003 support only one active network location type at a time. Windows automatically selects the network location type for the least secure network so that it can apply the profile that provides the maximum amount of protection. For example, if a computer has two active connections, one to a public network and one to a private network, Windows selects the public network type and applies it to all network adapters on the computer to enable the more rigorous security rules in its profile to protect the computer.

The Windows Firewall that is available in Windows XP and Windows Server 2003 support a domain profile that is identical in concept to the one described previously. However, instead of supporting both a private and public profile, these earlier versions of Windows support only a 'standard' profile. So if you create rules by using the Windows Firewall node in the Administrative Templates section of the Group Policy editor then you can only specify that they apply to the domain and standard profiles. If you specify the standard profile and then apply these rules to a computer that is running Windows Vista or later version of Windows, then the rules apply when the computer’s network location profile is set to either private or public. The rules in the domain profile still apply only when the computer’s network location profile is set to domain.

For more information about network location awareness and its use in Windows Firewall with Advanced Security, see the section "Network location-aware host firewall" in [Getting Started with Windows Firewall with Advanced Security](http://go.microsoft.com/fwlink/?linkid=64343) at http://go.microsoft.com/fwlink/?linkid=64343.

Next topic: [Host Firewall](#z4eb905238d874b79a7ef4a6a1fe4e513)

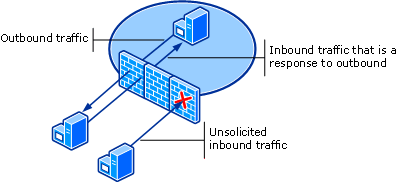
Host Firewall

Windows Firewall with Advanced Security includes a host-based firewall component that is a protective boundary for the local computer, which monitors and restricts information that travels between your computer and its attached networks or the Internet. It provides an important line of defense against someone who might try to access your computer without your permission.

In Windows Vista and later versions of Windows, both client and server, the host firewall in Windows Firewall with Advanced Security is turned on by default, with unsolicited inbound network traffic blocked, and all outbound traffic allowed. You can create rules to permit specific inbound connections if your computer hosts a service or program that must be able to receive inbound unsolicited network traffic. To control outbound network traffic you can create outbound block rules that prevent unwanted network traffic from being sent to the network. Alternatively, you can configure the default outbound behavior to block all traffic, and then create outbound allow rules that permit only that traffic that you configure in the rules.

How the host firewall works

Network traffic flowing in and out of your computer can be categorized as shown in the following diagram.



Network traffic consists of a packet or a stream of packets that are sent from a source port on one computer to a destination port on another computer. A port is just an integer value in the network packet that identifies the program on the sending or receiving end of the connection. Generally, only one program listens on a port at a time. To listen on a port, the program registers itself and the port numbers to which it must listen with the operating system. When a packet arrives at the local computer, the operating system examines the destination port number, and then provides the contents of the packet to the program registered to use that port. When using the TCP/IP protocol, a computer can receive network traffic addressed by using a specific transport protocol such as TCP or UDP, and on any one of the ports numbered from 1 to 65,535. Many of the lower numbered ports are reserved for well-known services, such as a Web server that uses Hyper Text Transport Protocol (HTTP) on TCP port 80, Telnet remote terminal services on TCP port 23, or Simple Mail Transfer Protocol (SMTP) on port 25.

Windows Firewall with Advanced Security works by examining the source and destination addresses, source and destination ports, and protocol numbers of a packet, and then comparing them to the rules that are defined by the administrator. When a rule matches a network packet then the action specified in the rule (to allow or block the packet) is taken. Windows Firewall with Advanced Security also lets you allow or block network packets based on whether they are protected by IPsec authentication or encryption.

For more information about host firewall functionality and the features of Windows Firewall with Advanced Security, see the [Windows Firewall with Advanced Security Getting Started Guide](http://go.microsoft.com/fwlink/?linkid=64343) in the Windows Server Technical Library at http://go.microsoft.com/fwlink/?linkid=64343, and [Windows Firewall](http://go.microsoft.com/fwlink/?linkid=95393) on TechNet at http://go.microsoft.com/fwlink/?linkid=95393.

Next topic: [Connection Security and IPsec](#z7336450e2796477abc55201bb0a10d7c)

Connection Security and IPsec

Internet Protocol Security (IPsec) is a framework of open standards for protecting communications over TCP/IP networks by using cryptographic security services. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on standards developed by the [Internet Engineering Task Force (IETF)](http://go.microsoft.com/fwlink/?LinkID=98592) IPsec working group.

The implementation of IPsec included with Windows Vista and later versions of Windows is fully integrated into the Network layer (layer 3) of the Open Systems Interconnection (OSI) network reference model. This lets it provide protection to any IP-based protocol in a manner that is transparent to the programs that are running on the computer. It fully supports both IPv4 and IPv6.

IPsec is an important layer in a defense-in-depth strategy to protect your organization's network-accessible resources.

How IPsec works

IPsec provides a variety of connection security services to network traffic. You can configure each service to apply to specific network traffic by creating a connection security rule in Windows Firewall with Advanced Security that identifies the characteristics of the network traffic to protect, and the nature of the protection to be applied.

 Source authentication. Source authentication ensures that each computer participating in a connection receives proof that the remote computer (and optionally the user on the remote computer) is truly the entity that it claims to be.

Authentication involves each computer providing some form of credentials to the other computer that can be proved to be from the claimed source. Kerberos tokens, which can be checked with a domain controller, or a computer or user certificate which can be cryptographically checked against its trusted root certificate, are among the authentication methods generally used.

 Data integrity. Data integrity ensures that the packet that is received is identical to the packet that was transmitted, and provides an assurance that it was not damaged or modified in transit.

A network packet that is sent through an IPsec protected connection includes a cryptographic hash of the packet. The hash is calculated by the sending computer, encrypted, and included in the packet. The receiving computer calculates its own hash on the received packet, and after decrypting the included hash, compares the two hash values. If they match, the packet is accepted and processed. If they do not match, then the packet was damaged or modified in transit, and is dropped.

 Data confidentiality. Data confidentiality ensures that the information included in the network connection cannot be accessed or read by non-authorized computers or users.

When enabled, every network packet sent through the protected connection has its data payload encrypted. Various strength encryption protocols are available for use. Protocols that provide a greater level of protection generally require more computer resources to process the more complex cryptographic algorithms.

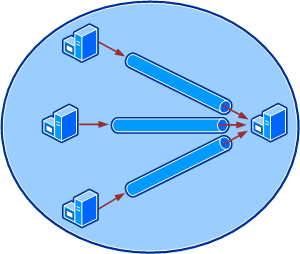
Transport versus Tunnel Mode

IPsec operates in one of two modes: transport or tunnel mode.

Transport mode. In transport mode, the network traffic is IPsec-protected by the originating computer and it stays protected all of the way through the network to the destination computer. The IPsec-protected packets are routed to their destination as standard IP datagrams by the routers along the way. Transport mode provides end-to-end security. A transport mode connection security rule requires only two IP addresses: the source and destination computers. The domain and server isolation scenarios discussed in this guide use transport mode IPsec rules.

The following diagram illustrates transport mode, where each computer establishes an iPsec protected connection from itself to a remote server.

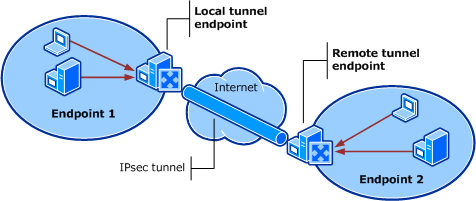
Transport mode IPsec



Tunnel mode. In tunnel mode, the network traffic is IPsec-protected only for a part of the trip between the origin and destination computers, typically as it traverses an untrusted network. For example, an organization with two geographically separated private intranets that are separated by Internet, can use an IPsec tunnel mode connection to treat the two separate intranets as one logical network. To do this, a computer on each intranet is designated as the IPsec gateway, or tunnel endpoint. Clients and servers in each intranet treat their local gateway as a router. But instead of routing packets across the Internet like a typical router, the gateway creates an IPsec-protected connection, or tunnel, and then sends the packets through the tunnel. Traffic is sent plain text between the client and the local gateway, then sent IPsec-protected from the local gateway to the remote gateway, and then finally sent plain text again between the remote gateway and the destination computer. Unlike a transport mode rule, a tunnel mode rule requires four IP addresses: the two tunnel endpoints, or gateway computers, and the two sets of computers that are accessible to each other through the tunnel, referred to as endpoints. The endpoints are typically sets of subnet addresses.

The following diagram illustrates tunnel mode, where computers on each intranet can communicate with computers on the other intranet by routing packets through the IPsec tunnel between the two gateways.

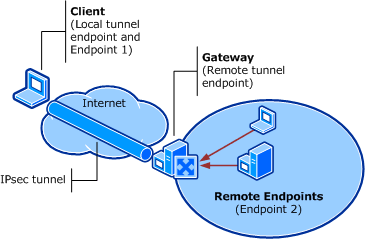
Tunnel mode IPsec between two gateways



Tunnel mode can also be used in a scenario where the originating computer is the local gateway. This is a typical VPN scenario, where the client computer is attached to an untrusted network, but communicates securely with computers on a private intranet through an IPsec tunnel established with a remote gateway. In this case, one of the endpoints and its corresponding tunnel endpoint are one and the same.

The following diagram illustrates a tunnel mode connection between a remote client and an IPsec gateway to a private network.

Tunnel mode IPsec between a client and a gateway



You can also combine the tunnel and transport mode rules, to have a client establish a tunnel mode connection to a remote site, and transport mode end-to-end protected connections to servers in that site. The transport mode traffic is sent through the tunnel as is all other traffic between the client and the site.

For more information about IPsec, see:

 [Windows Firewall with Advanced Security Getting Started Guide](http://go.microsoft.com/fwlink/?linkid=64343) at http://go.microsoft.com/fwlink/?linkid=64343.

 [Introduction to Server and Domain Isolation](http://go.microsoft.com/fwlink/?linkid=94631) at http://go.microsoft.com/fwlink/?linkid=94631

For more information about the IPsec functionality in Windows Firewall with Advanced Security and its use in supporting serer and domain isolation, see:

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

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

Next topic: [Group Policy](#z7863c88524e44ad79992b98b5fe843ab)

Group Policy

Group Policy enables you to perform your administrator tasks more efficiently because it enables centralized computer and user management. Centrally managing the configuration settings of the computers and users on the network can decrease the total cost of ownership for an IT infrastructure.

How Group Policy works

Group Policy is a technology available as part of an Active Directory Domain Services (AD DS) implementation. When domain member computers connect to their Active Directory domain, they automatically retrieve and apply Group Policy objects (GPOs) from the domain controller.

A GPO is a collection of settings that can be created by a domain administrator, and then applied to groups of computers or users in the organization.

Configuration settings and rules that you want to apply to the computers in your organization are stored in GPOs that are maintained on the domain controllers of an Active Directory domain. The GPOs are automatically downloaded to all assigned computers when they connect to the domain. They are then merged with the local GPO stored on the computer, and then applied to the computer's active configuration. Group Policy provides easy centralized management, and detailed control of which computers receive which GPOs.

Because the capabilities of both firewall rules and the implementation of IPsec are significantly enhanced in Windows Vista and later versions of Windows, we recommend that administrators leave existing GPO settings in place for earlier versions of Windows and create new GPOs for computers that are running versions of Windows with Windows Firewall with Advanced Security. By applying the new GPOs to the same set of containers as the old GPO settings, and by using WMI filters with each GPO as demonstrated in this guide, you can ensure that you apply the most appropriate settings to each computer in your organization. For example, create one GPO (or set of GPOs) to contain the firewall and IPsec policy configuration for Windows XP and Windows Server 2003 computers. Use WMI filters to ensure that these GPOs apply only to computers that are running those versions of Windows. Use a different GPO (or set of GPOs) to contain the firewall and connection security rules for computers that are running Windows 7, Windows Vista, Windows Server 2008 R2, and Windows Server 2008. Use WMI filters to ensure that these GPOs apply only to those computers that are running those versions of Windows.

For more information about Group Policy, see [Windows Server Group Policy](http://go.microsoft.com/fwlink/?linkid=93542) at http://go.microsoft.com/fwlink/?linkid=93542.

Next topic: [Requirements for Performing the Scenarios](#ze245fa7756ea4c13bb2d83ce018e5834)

Requirements for Performing the Scenarios

This section describes how to configure computers to try the scenarios for Windows Firewall with Advanced Security in a test lab environment. Step-by-Step guides are not necessarily meant to be used to deploy Windows Server features without accompanying documentation (as listed in the [Additional References](#ze4248de52d0747219c54163e351e33fb) section). Use this guide as a stand-alone document with discretion.

Caution

If you accidentally apply Windows Firewall with Advanced Security settings to a GPO that applies to production computers, you can affect their ability to communicate with other computers.

In this section:

 [Hardware requirements](#z1)

 [Software requirements](#z2)

 [Required common procedures](#z3)

 [Setting up the lab computers](#z4)

Hardware requirements

You must meet the following hardware requirements in order to set up the test lab:

 Three computers that can run the operating systems required for the roles used in this guide (see the "Software Requirements" section later in this guide). The computers can be physical computers attached to a physical network, or virtual computers that are running on Microsoft® Hyper-V Server, the Hyper-V server role in Windows Server 2008 R2 or Windows Server 2008, or Virtual Server or Virtual PC and connected to an isolated virtual network.

The computers needed for a test lab for this guide include the following:

a. DC1 is a computer that is running Windows Server 2008 R2 or Windows Server 2008, Standard or Enterprise Edition, configured to provide the following functions:

 The primary domain controller for the Contoso.com Active Directory domain

 A Domain Name System (DNS) server that can resolve names for the Contoso.com DNS zone

b. MBRSVR1 is a computer that is running Windows Server 2008 R2 or Windows Server 2008, Standard or Enterprise Edition, configured to provide the following functions:

 A domain member in the Contoso.com domain

 A manager and editor of the Group Policy objects in the Contoso.com domain

 A Telnet server

c. CLIENT1 is a computer that is running Windows 7 or Windows Vista, configured as follows:

 A domain member in the Contoso.com domain

 A Telnet client

 The computers must be connected to each other by using a network. We recommend that you use a stand-alone, isolated network that contains nothing but the computers that are used in this guide.

Caution

If you connect your test network to your production environment or to the Internet then we strongly recommend that you make sure that all computers are updated with the latest security updates and are running appropriate antivirus protection software.

Note

The steps in this guide assume that your computers are on an isolated test lab network, and that the names, IP addresses, and so on, do not interfere with the operation of other computers on your production environment.

Software requirements

 For DC1: Windows Server 2008 R2 or Windows Server 2008, Standard or Enterprise Edition.

 For MBRSVR1: Windows Server 2008 R2 or Windows Server 2008, Standard or Enterprise Edition.

 For CLIENT1: Windows 7 or Windows Vista.

Note

If you use Windows Server 2008 on MBRSVR1, or Windows Vista on CLIENT1 then you cannot perform the steps that demonstrate features unique to Windows Server 2008 R2 and Windows 7. These steps are clearly identified in the text.

Required common procedures

The procedures that are shown here frequently occur in this guide, and the steps for them are not included in-line. See the steps listed here any time that you must refer to them.

Responding to the User Account Control dialog box

The User Account Control dialog box can appear when you try to perform a task that requires administrative permissions. If your account is a member of the local Administrators group then you can click Continue when you are prompted. If your user account is not an administrator then you must provide the credentials (user name and password) of an account that has the required permissions.

Note

User Account Control dialog boxes appear much less frequently in Windows 7 and Windows Server 2008 R2 than in earlier versions of Windows.

Administrator command prompts

Use the following procedure when you are instructed to open an Administrator: Command prompt.

To open an Administrator: Command prompt

|  |
| --- |
| 1. Click Start, click All Programs, and then click Accessories.  2. Right-click Command Prompt, and then click Run as administrator.  You can do the same thing with any shortcut to the command prompt that you put in the Start menu, or on the desktop, or that you pin to the taskbar or Quick Launch bar. |

Starting Windows Firewall with Advanced Security

Use the following procedure when you are instructed to open the Windows Firewall with Advanced Security MMC snap-in.

To open the Windows Firewall with Advanced Security MMC snap-in

|  |
| --- |
|  Click Start, in the Start Search box, type wf.msc, and then press ENTER.  Alternatively:   On Windows Server 2008 R2 or Windows Server 2008 you can click Start, click Administrative Tools, and then click Windows Firewall with Advanced Security. |

Setting up the lab computers

First, set up the domain controller and create the domain that has the required user accounts.

To install and configure the domain controller DC1

|  |
| --- |
| 1. Install Windows Server 2008 R2 or Windows Server 2008 by using the following settings:  2. Set the local Administrator account password to Pass@word1.  3. Configure the network to use the following settings:   IP address: 192.168.0.1   Subnet mask: 255.255.255.0   Default gateway: Leave blank   DNS server address: 192.168.0.1  4. Name the computer DC1. Restart the computer when you are prompted.  5. Install Active Directory by using the following settings:   Create a new domain in a new forest, and name the domain contoso.com.   Set the Forest Functional Level to the highest level supported in the version of Windows Server that you are using.   Include DNS as part of the installation.   Use the password Pass@word1 for all user accounts.  6. After installing Active Directory, restart the computer when you are prompted.  7. Create a new user account in Contoso named Admin1, with a password of Pass@word1.  8. Add Admin1 to the group Domain Admins. |

Now install the member server, and then configure the required services.

To install and configure the member server MBRSVR1

|  |
| --- |
| 1. Install Windows Server 2008 R2 or Windows Server 2008 by using the following settings:  2. Set the local Administrator account password to Pass@word1.  3. Configure the network to use the following settings:   IP address: 192.168.0.100   Subnet mask: 255.255.255.0   Default gateway: Leave blank   DNS server address: 192.168.0.1  4. Name the computer MBRSVR1, join the computer to the contoso.com domain, and then restart the computer when you are prompted.  5. Use Server Manager to install the features Group Policy Management and Telnet Server onto the computer.  6. Use the Services.msc console to configure the Telnet service to start automatically whenever the computer starts, and then start the service. |

Finally, install the workstation client, and configure it.

To install and configure the client computer CLIENT1

|  |
| --- |
| 1. Install Windows 7 or Windows Vista by using the following settings:  2. When prompted to name the local administrator during setup, name it localadmin, and then set its password to Pass@word1.  3. Name the computer CLIENT1.  4. Identify the network location type as Work.  5. Configure the network to use the following settings:   IP address: 192.168.0.101   Subnet mask: 255.255.255.0   Default Gateway: Leave blank   DNS server address: 192.168.0.1  6. Using the Turn Windows features on and off option in the Program and Features control panel program, install the Telnet Client onto the computer.  7. Join the computer to the contoso.com domain, and then restart the computer when you are prompted. |

Next topic: [Examining Default Settings on Clients and Servers](#zb872d80528684fe5b0af5abc5549729a)

Examining Default Settings on Clients and Servers

The functionality provided by Windows Firewall with Advanced Security can be accessed by using three different user interfaces:

 Windows Firewall in Control Panel. This interface provides access to only basic host firewall settings and is intended for a consumer in a non-managed environment. The Windows Firewall icon in Control Panel has limited functionality and is designed for consumer control of a single computer, instead of enterprise administrator control over lots of computers.

 Netsh Advfirewall command-line tool. The netsh command provides the ability to modify many aspects of a computer's network configuration in a scriptable manner at a command prompt. This includes the ability to configure the Windows Firewall with Advanced Security settings and rules for a single computer, or for a domain Group Policy object (GPO) that can be applied to many computers in an enterprise environment.

 Windows Firewall with Advanced Security Microsoft Management Console (MMC) snap-in. This interface provides access to both firewall and IPsec functionality, and is the primary means for an administrator to manage both an individual computer and a GPO. The MMC snap-in is not designed for a home user, but for the enterprise administrator.

Each of these provides different abilities. The Windows Firewall Control Panel program is significantly restricted because of its target audience of home consumers.

The Windows Firewall with Advanced Security MMC snap-in and the netsh command-line tool have very similar capabilities, but there are still some differences. They are discussed in this section.

Steps for examining default settings on clients and servers

In this section of the guide, you learn how to start each tool to see what functionality is available through it. By using each of these tools you see the default and current configuration in Windows Firewall with Advanced Security for computers that are running Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008.

[Step 1: Starting Windows Firewall in Control Panel](#z059301885e9b4e4db1342940519d0efd)

[Step 2: Examining the Basic Options Available by Using the Control Panel Interface](#zb70ca22ab359405d90cd4d564df28281)

[Step 3: Examining the Basic Options by Using the Netsh Command-Line Tool](#z20937ecd7005477db4596f73e86c8240)

[Step 4: Examining the Basic Options Available When Using the Windows Firewall with Advanced Security MMC snap-in](#zb799c1490c19432a924095a4e65304d8)

[Step 5: Examine the Differences in Functionality Between the MMC Snap-in and the Netsh Command-line Tool](#z47f43fe9c5fd4bb894451149855751d8)

Next topic: [Step 1: Starting Windows Firewall in Control Panel](#z059301885e9b4e4db1342940519d0efd)

Step 1: Starting Windows Firewall in Control Panel

In this step, you open the Windows Firewall icon in Control Panel on each of your domain member computers.

To open Windows Firewall in Control Panel on CLIENT1

|  |
| --- |
| 1. On CLIENT1, log on as contoso\admin1 with the password Pass@word1.  2. Click Start, and then click Control Panel.  In Windows 7, the default Control Panel view is View by: Category. In Windows Vista, the default view is Control Panel Home. The steps that follow assume that you are using the default view.  3. Click System and Security (Windows 7) or Security (Windows Vista), and then click Windows Firewall.  4. On the Windows Firewall page, note the following default settings that are part of a typical installation, as shown in the following figures:   Windows Firewall is enabled on all profiles.   Unsolicited inbound connections that do not have an exception are blocked.   When a program tries to listen for incoming connections and is prevented from doing this by the firewall, a notification is displayed to the user.   The current settings are those assigned to the Domain network location profile because the computer is joined and authenticated to an Active Directory domain.  Default options in Windows 7:    Default options in Windows Vista:    5. Keep Windows Firewall in Control Panel open. |

Now examine the same interface on Windows Server.

To open Windows Firewall in Control Panel on MBRSVR1

|  |
| --- |
| 1. On MBRSVR1, log on as contoso\admin1 with the password Pass@word1.  2. Click Start, and then click Control Panel.   In Windows Server 2008 R2, the default Control Panel view is View by: Category. Click System and Security and then click Windows Firewall.   In Windows Server 2008, the default Control Panel view is Classic View. Click Windows Firewall.  3. On the Windows Firewall page, note the following default settings that are part of a typical Windows Server installation:   Windows Firewall is enabled on all profiles.  Note  If the computer that is running Windows Server was upgraded from an earlier version of Windows Server that included Windows Firewall then the On/Off state is preserved in the upgrade.   Unsolicited inbound connections that do not have an exception are blocked.   When a program tries to listen for incoming connections and is prevented from doing this by the firewall, a notification is not displayed to the user.  Note  This differs from the default setting on Windows 7 or Windows Vista.   The current settings are those assigned to the Domain network location profile because the computer is joined to a domain and authenticated.  4. Keep Windows Firewall in Control Panel open. |

Next topic: [Step 2: Examining the Basic Options Available by Using the Control Panel Interface](#zb70ca22ab359405d90cd4d564df28281)

Step 2: Examining the Basic Options Available by Using the Control Panel Interface

In this step, you examine the options that you can configure by using the Windows Firewall icon in Control Panel, and compare the differences between the client and server versions of Windows.

To examine the options available in the Windows Firewall icon in Control Panel

|  |
| --- |
| 1. Perform the following step two times, once for CLIENT1, and then once for MBRSVR1:   If the computer is running Windows 7 or Windows Server 2008 R2, and then, in the left-hand list of tasks, click Turn Windows Firewall on or off.  On the Customize Settings page you can you can enable or disable the firewall for each network location profile. In addition, you can choose to block all incoming connections, even when an exception rule exists that ordinarily allows a connection. The Customize Settings page also lets you specify, also on a per-profile basis, whether the firewall notifies you when it blocks a new program and offers you the opportunity to allow the program. Choosing to allow the program creates a program exception rule for that program.  Click Cancel to close the Customize Settings page when you have finished examining it.   If the computer is running Windows Vista, click Change settings, and examine the General tab.  On the General tab, you can enable or disable the firewall. In addition, you can choose to block all incoming connections, even when an exception rule exists that ordinarily allows a connection. To change the notification settings, you must select the Exceptions tab, and select or clear Notify me when Windows Firewall blocks a new program at the bottom of the dialog box. Remember that in Windows Vista or Windows Server 2008, changes that you make here apply only to the currently configured network location profile (Domain network).  Close the dialog box when you have finished examining it.  Caution  Do not disable the firewall by stopping the Windows Firewall (MpsSvc) service. Because the Windows Firewall service also implements Windows Service Hardening, which provides additional protections for other Windows services, Microsoft does not support disabling the Windows Firewall service. Instead, use the interface shown here in the Windows Firewall icon in Control Panel or use the Windows Firewall with Advanced Security MMC snap-in. For more information about Windows Service Hardening, see [Windows Vista Security and Data Protection Improvements](http://go.microsoft.com/fwlink/?linkid=98656) at http://go.microsoft.com/fwlink/?linkid=98656.  Disabling the firewall by using the Off setting on the Windows Firewall Settings page does not stop the Windows Firewall (MpsSvc) service. It does stop Windows Firewall from filtering any inbound or outbound network traffic according to the configured rules.  2. Perform the following step two times, once for CLIENT1, and then once for MBRSVR1:   If the computer is running Windows 7 or Windows Server 2008 R2, then, in the left-hand list of tasks, click Allow a program or feature through Windows Firewall.  On the Allowed Programs page you can view and modify the list or programs that are permitted to listen for and receive network packets from the network. To see more information about an exception, select the row by clicking the rule name (do not check a box on the row) and then clicking Details. For each program, you can specify which network location profiles use the exception rule by selecting or clearing the boxes in the Domain, Home/Work (Private), or Public columns.  Click Cancel to close the Allowed Programs page when you have finished examining it.   If the computer is running Windows Vista or Windows Server 2008, click Change settings, and examine the Exceptions tab.  On the Exceptions tab you can view and modify the list of programs that are permitted to listen for and receive network packets from the network. The selected exceptions are enabled. Most of the entries displayed here represent predefined rule sets that are included with Windows. If you click the name of an exception and then click Properties, a description of the exception appears. You can also create your own custom program-based and port-based exceptions on this page. You can specify a scope to an exception: any computer, the local subnet only, or a custom list of addresses and subnets.  Close the dialog box when you have finished examining the Exceptions tab.  A computer that is running Windows Server and configured to have a network server role, such as a domain controller, typically has many more exceptions enabled to allow access to its services than a computer that is running a client version of Windows. For example, the MBRSVR1 computer has the Telnet exception rule enabled because you installed that service as part of the setup for this guide. The rule was created and enabled automatically during the installation of the Telnet service.  3. On both CLIENT1 and MBRSVR1, close the Windows Firewall page, and then close Control Panel. |

Next topic: [Step 3: Examining the Basic Options by Using the Netsh Command-Line Tool](#z20937ecd7005477db4596f73e86c8240)

Step 3: Examining the Basic Options by Using the Netsh Command-Line Tool

In this step, you try an alternative method for seeing the basic firewall configuration options by using the Netsh command-line tool.

To examine the basic firewall options by using Netsh

|  |
| --- |
| 1. On MBRSVR1, open an administrator command prompt.  2. At the command prompt, run netsh advfirewall show currentprofile.  Important  You must use the advfirewall context instead of the older firewall or ipsec contexts. Advfirewall was added to the netsh command in Windows Vista and is also present in later versions. The firewall and ipsec contexts still exist, but are provided only for compatibility with Group Policy settings created by using an earlier version of Windows.  In Windows 7 and Windows Server 2008 R2, the firewall context is obsolete and generates a warning message whenever you use it.  3. Examine the output and compare to what you saw earlier in the Windows Firewall icon in Control Panel. Your output resembles the following figure.    The values State, Firewall Policy, and InboundUserNotification correspond to the basic settings that you examined in the Windows Firewall Control Panel program in the previous steps. The other settings shown in the netsh output are not configurable by using the Windows Firewall Control Panel program. They are configurable by using the netsh command-line tool, and the Windows Firewall with Advanced Security MMC snap-in.  Note  In Windows 7 and Windows Server 2008 R2, if multiple network profiles are active on the computer because of it being connected to multiple networks then the output of the show currentprofile command includes a section for each active profile.  4. At the command prompt, run netsh advfirewall show global. This command displays some of the global (non-profile and non-rule specific) configuration settings for the firewall and IPsec. It includes, among other things, the default main mode negotiation proposals. These settings can be configured by using the netsh advfirewall set global command. The main mode defaults can also be configured in the Windows Firewall with Advanced Security MMC snap-in on the Windows Firewall with Advanced Security Properties page, on the IPsec Settings tab, under IPsec defaults.  5. Close the command prompt. |

Next topic: [Step 4: Examining the Basic Options Available When Using the Windows Firewall with Advanced Security MMC snap-in](#zb799c1490c19432a924095a4e65304d8)

Step 4: Examining the Basic Options Available When Using the Windows Firewall with Advanced Security MMC snap-in

In this step, you use the Windows Firewall with Advanced Security MMC snap-in to see the basic options available.

To examine the basic options by using the Windows Firewall with Advanced Security MMC snap-in

|  |
| --- |
| 1. On MBRSVR1, open Windows Firewall with Advanced Security.  2. Examine the three panes of the Windows Firewall with Advanced Security snap-in.   The navigation pane enables you to select from the main functional areas.   The results pane displays information about currently selected functional area.   The actions pane displays tasks that are relevant to the currently selected functional area.  3. In the navigation pane, select the node labeled Windows Firewall with Advanced Security.  The results pane displays the basic state information for each network location profile. Because MBRSVR1 is connected to the domain, the entry for that network location profile in the Overview section reads Domain Profile is Active.  Note  In Windows 7 and Windows Server 2008 R2 more than one profile can be listed as active, if there are connections to multiple networks.  4. In the navigation pane, right-click Windows Firewall with Advanced Security, and then click Properties.  5. Note that there are four tabs, one for each network location profile and one for IPsec settings. The changes you make on each profile tab only apply to the computer when the specified network location profile is active. The IPsec Settings tab enables you to configure the default IPsec protocol parameters that are used when a connection security rule does not specify otherwise.  6. Click the Private Profile tab as an example. Note that for each profile, you can enable or disable the firewall, configure the default firewall behavior for handling unsolicited inbound connections and outbound connections, and specify logging options.  7. Click Customize in the Settings section. Note that for each profile, you can configure notifications and how your computer responds to incoming multicast or broadcast network traffic.  The Rule merging section is disabled because they apply only when you are managing the settings of a Group Policy object (GPO) instead of the local computer. These settings indicate whether the GPO allows local Administrators to apply their own locally created firewall and connection security rules. If set to No then only GPO-supplied rules are applied to the computer and any locally defined rules are ignored.  8. Click Cancel to return to the main Properties dialog box.  9. Click Customize in the Logging section to examine the options available for creating a log file to capture details about the firewall's operation. Even though a log file name is specified, nothing is written to the file until you select Yes in one of the two lists.  10. Set the value of both lists to No to disable logging. You will use this in a later section of the guide.  11. Click Cancel two times to return to the Windows Firewall with Advanced Security snap-in.  12. You can select the other functional areas to see the currently configured Inbound Rules, Outbound Rules, and Connection Security Rules, but do not change any settings at this point. |

Next topic: [Step 5: Examine the Differences in Functionality Between the MMC Snap-in and the Netsh Command-line Tool](#z47f43fe9c5fd4bb894451149855751d8)

Step 5: Examine the Differences in Functionality Between the MMC Snap-in and the Netsh Command-line Tool

In this topic, you examine the differences between the Windows Firewall with Advanced Security MMC snap-in, and the netsh command-line tool. The following table identifies features supported in Windows 7 and Windows Server 2008 R2 that can be configured either in the MMC snap-in or the netsh command-line tool, but not both. The table identifies how to find the option in the snap-in, or which netsh option implements the feature. Do not modify any of these settings at this point.

|  |  |  |
| --- | --- | --- |
| Features | Windows Firewall with Advanced Security MMC snap-in support | Netsh support |
| Configure the global IPsec quick mode default settings. These settings are used when a connection security rule does not specify otherwise. | On the Windows Firewall with Advanced Security Properties dialog box, on the IPsec Settings tab, under IPsec defaults, click Customize, and then under Data protection (Quick Mode), select Advanced and then click Customize. | You cannot use netsh to configure the global quick mode default settings. |
| Configure the global IPsec main mode default settings. The global default settings are used when a connection security rule does not specify its own main mode settings, and a separate main mode rule (Windows 7 or Windows Server 2008 R2 only) does not match the connection. | On the Windows Firewall with Advanced Security Properties dialog box, on the IPsec Settings tab, under IPsec defaults, click Customize, and then under Key Exchange (Main Mode), select Advanced and then click Customize. | You cannot use netsh to configure the global main mode default settings. |
| Configure which network connections are protected by each profile. If the check box for a network connection is cleared then that network connection is not protected by the profile even if the attached network matches that network location type. | On the Windows Firewall with Advanced Security Properties dialog box, under any of the Profile tabs, next to Protected network connections, click Customize. | You cannot use netsh to configure per profile enabling or disabling of specific connection types. |
| Create main mode rules that specify authentication settings for connections between specified IP addresses, or for connections using specific network location profiles. If a connection matches a main mode rule then it is used instead of the global default settings, or even the settings specified in the connection security rule. Main mode rules are supported on Windows 7 and Windows Server 2008 R2 only. | You cannot use the MMC snap-in to create main mode rules. | Use the netsh advfirewall mainmode add rule command. |
| Create a connection security rule that uses a specific quick mode configuration instead of the global defaults. | You cannot use the MMC snap-in to create rules with per-rule quick mode settings. Rules created in the MMC snap-in, they always use the global quick mode default settings. | Use the qmsecmethods parameter of the netsh advfirewall consec add rule command. |
| Create a rule that specifies that Perfect Forward Secrecy (PFS) is used in Quick Mode negotiations. | You cannot use the MMC snap-in to create rule that specifies quick mode PFS. | Use the qmpfs parameter of the netsh advfirewall consec add rule command. |
| Configure how the computer performs certificate revocation list (CRL) checking. | You cannot use the MMC snap-in to change the configuration for strong CRL checking. | Use the strongcrlcheck parameter of the netsh advfirewall set global command. |
| Configure the time-out value for an IPsec security association (SA). | You cannot use the MMC snap-in to configure the IPsec SA time-out. | Use the saidletimemin parameter of the netsh advfirewall set global command. |
| Specify whether IPv6 Neighbor Discovery protocol is exempted from the requirements of IPsec. | You cannot use the MMC snap-in to configure a global IPsec exemption for the IPv6 Neighbor Discovery protocol. | Use the neighbordiscovery value in the defaultexemptions parameter of the netsh advfirewall set global command. |
| Specify whether DHCP is exempted from the requirements of IPsec. | You cannot use the MMC snap-in to configure a global IPsec exemption for the DHCP protocol. | Use the dhcp value in the defaultexemptions parameter of the netsh advfirewall set global command. |
| Configure a connection security rule that matches UDP packets that contain embedded Teredo packets. | You cannot use the MMC snap-in to configure a firewall rule that matches Teredo packets. | Use the teredo value in the localport parameter of the netsh advfirewall firewall add rule command. |
| Configure Windows Firewall with Advanced Security to allow remote management. | You cannot use the MMC snap-in to enable remote management of Windows Firewall with Advanced Security. | Use the remotemanagement option of the netsh advfirewall set domainprofile settings command. |
| When configuring a Group Policy that contains a list of users or computers that are authorized to use an IPsec tunnel, remove the list and set the effective setting back to “Not configured”. | You cannot use the MMC snap-in, when you are managing a GPO, to set IPsec tunnel authorization for users and computers back to “Not configured”. | Use the authzusergrp and authzcomputergrp options in the netsh advfirewall set global ipsec command, and set each to the value of notconfigured. |

Next topic: [Deploying Basic Settings by Using Group Policy](#z814a075710a14b38a141b76332482e1c)

Deploying Basic Settings by Using Group Policy

You can use Group Policy to define and deploy specific configurations for groups of users and computers. These configurations are created by using the Group Policy Management Editor and are contained in one or more Group Policy objects (GPOs) stored in Active Directory. To deploy the settings, the GPO is linked to one or more Active Directory containers, such as a site, a domain, or an organizational unit (OU). The settings in the GPO are then applied automatically to the users and computers whose objects are stored in those Active Directory containers. You can configure the work environment for your users once, and then rely on Group Policy to enforce your settings.

For an overview of Group Policy, see the [Group Policy](#z7863c88524e44ad79992b98b5fe843ab) technology review in this guide. For more information about Group Policy, see [Windows Server Group Policy](http://go.microsoft.com/fwlink/?linkid=93542) at http://go.microsoft.com/fwlink/?linkid=93542.

Steps for deploying basic settings by using Group Policy

In this section, you create a set of OUs to contain your computer accounts. You then create GPOs that contain settings that are intended for a specific set of computers. You use the Group Policy Management Editor to configure a GPO that contains basic firewall settings, and then assign that GPO to the OU that contains your test computer. Finally, you create and apply a Windows Management Instrumentation (WMI) filter to restrict the application of the GPO to computers that are running a specified version of Windows. This enables you to have multiple groups of computers in a single Active Directory container (OU, site, or domain) that require different settings, and ensure that each receives the correct GPO.

The GPOs that you configure include some of the basic Windows Firewall with Advanced Security settings that are part of typical enterprise firewall settings.

[Step 1: Creating OUs and Placing Computer Accounts in Them](#za4fce227dd3144e99524e53b22cd86c8)

[Step 2: Creating the GPOs to Store Settings](#z122da304b3c247f496e8ebc7b118e55b)

[Step 3: Adding the GPO Setting to Enable the Firewall on Member Client Computers](#z07a85134f0054d2ea2b787781fbde9f9)

[Step 4: Deploying the Initial GPO with Test Firewall Settings](#zdaaf9da2ae9c4d87ac352462be2595f9)

[Step 5: Adding the Setting that Prevents Local Administrators from Applying Conflicting Rules](#zce3e26ed04a84b84aa687e0844236484)

[Step 6: Configuring the Rest of Your Client Computer Firewall Settings](#z1bf9b554d6194b1ea26dc5e891b9ede1)

[Step 7: Creating WMI and Group Filters](#z683088705d17423abcb5aa1108933cdf)

[Step 8: Enabling Firewall Logging](#z6c16ece5dfd84ac09deb93080294e38f)

Next topic: [Step 1: Creating OUs and Placing Computer Accounts in Them](#za4fce227dd3144e99524e53b22cd86c8)

Step 1: Creating OUs and Placing Computer Accounts in Them

In this step, you use the Active Directory Users and Computers MMC snap-in to create two OUs in your domain hierarchy: one for member servers, and one for member client computers. You then move each computer account to the relevant new OU.

To create your OUs and put your computer accounts in them

|  |
| --- |
| 1. On DC1, click Start, click Administrative Tools, and then click Active Directory Users and Computers.  Note  You can also run this tool on member servers or domain-joined client computers if you first install the [Remote Server Administration Tools](http://go.microsoft.com/fwlink/?linkid=157183) (http://go.microsoft.com/fwlink/?linkid=157183) from the Microsoft Download Center.  Alternatively, you can use Server Manager. Expand Roles, expand Active Directory Domain Services, and then expand Active Directory Users and Computers [DC1.contoso.com].  2. In the navigation pane, right-click contoso.com, click New, and then click Organizational Unit.  3. In the Name box, type MyMemberServers, and then click OK.  4. Right-click contoso.com again, and then click New, and then click Organizational Unit.  5. In the Name box, type MyClientComputers, and then click OK.  6. In the navigation pane, click Computers.  7. In the results pane, right-click CLIENT1, and then click Move.  8. In the Move dialog box, click MyClientComputers, and then click OK.  9. In the results pane, right-click MBRSVR1, and then click Move.  10. In the Move dialog box, click MyMemberServers, and then click OK.  When you have finished, your display resembles the following figure.    11. Close the Active Directory Users and Computers snap-in. |

Next topic: [Step 2: Creating the GPOs to Store Settings](#z122da304b3c247f496e8ebc7b118e55b)

Step 2: Creating the GPOs to Store Settings

In this step, you create a new GPO. Because it is not yet linked to any OU, the settings that you configure do not yet apply to any computers.

To create the GPOs

|  |
| --- |
| 1. On MBRSVR1, click Start, click Administrative Tools, and then click Group Policy Management.  Alternatively, if you use Server Manager, expand Features, and then expand Group Policy Management.  2. In the navigation pane, expand Forest: contoso.com, expand Domains, and then expand contoso.com.  3. In the navigation pane, right-click Group Policy Objects, and then click New.  4. In the Name box, type Firewall Settings for Windows Servers, and then click OK.  5. In the navigation pane, right-click Group Policy Objects, and then click New.  6. In the Name box, type Firewall Settings for Windows Clients, and then click OK.  7. Select the Group Policy Objects node, and your display resembles the following figure. |

Next topic: [Step 3: Adding the GPO Setting to Enable the Firewall on Member Client Computers](#z07a85134f0054d2ea2b787781fbde9f9)

Step 3: Adding the GPO Setting to Enable the Firewall on Member Client Computers

In this step, you configure your client GPO to include a setting that enables Windows Firewall on all your client computers that are running Windows 7 or Windows Vista to which the GPO applies.

To add the GPO setting to enable the firewall on member client computers

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management, click Group Policy Objects, right-click Firewall Settings for Windows Clients, and then click Edit.  2. In Group Policy Management Editor, right-click the top node Firewall Settings for Windows Clients [DC1.contoso.com] Policy, and then click Properties.  3. Select the Disable User Configuration settings check box.  Note  We recommend that you remove the user or computer sections in any GPO in which they are not used. This improves performance on the client computer when it is applying a GPO.  4. In the Confirm Disable dialog box, click Yes, and then click OK.  5. Under Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, and then expand Windows Firewall with Advanced Security.  6. Click the node Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com, where GUID is a unique number assigned to your domain.  7. In the results pane, under Overview, notice that for each network location profile Windows Firewall state is not configured, and then click Windows Firewall Properties.  8. On the Domain Profile tab, click the drop-down list next to Firewall state, and then click On (recommended).  Note  This might appear to be an unnecessary step, because the firewall is turned on by default on the client computers. However, if you leave this setting as Not configured, a local administrator can disable the firewall. Setting it in the GPO as shown in this step turns it on and prevents the local administrators from disabling it.  9. Click OK to save your changes. Note in the results pane that Domain Profile now shows Windows Firewall is on.    10. Close Group Policy Management Editor. |

Next topic: [Step 4: Deploying the Initial GPO with Test Firewall Settings](#zdaaf9da2ae9c4d87ac352462be2595f9)

Step 4: Deploying the Initial GPO with Test Firewall Settings

In this step, you link your GPO to an OU to apply it to your domain-joined client computer.

To deploy your firewall settings

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management, in the navigation pane, right-click MyClientComputers, and then click Link an Existing GPO.  2. In the Group Policy objects list, click Firewall Settings for Windows Clients, and then click OK. |

In the next procedure, you confirm that the client computer receives and applies the new GPO settings.

To test your new GPO

|  |
| --- |
| 1. On CLIENT1, open an administrator command prompt.  2. At the command prompt window, type gpupdate /force, and then press ENTER. Wait until the command finishes before moving to the next step.  3. To validate that the GPO was correctly applied, run gpresult /r /scope computer. In the output, look for the section Applied Group Policy Objects. Confirm that it contains entries for both Firewall Settings for Windows Clients and the Default Domain Policy.  4. Open the Windows Firewall with Advanced Security snap-in.  5. Right-click the top node Windows Firewall with Advanced Security on Local Computer, and then click Properties.  6. Note that the Firewall State setting is On (recommended), and that the list control is disabled. It is now controlled by Group Policy and cannot be changed locally, even by an administrator.  7. Close the Properties dialog box, and the Windows Firewall with Advanced Security snap-in. |

Next topic: [Step 5: Adding the Setting that Prevents Local Administrators from Applying Conflicting Rules](#zce3e26ed04a84b84aa687e0844236484)

Step 5: Adding the Setting that Prevents Local Administrators from Applying Conflicting Rules

In this step, you configure and test a setting that prevents firewall rules created by local administrators from being applied to the computer and possibly conflicting with the GPO-deployed rules.

By default members of the local Administrators group on the computer can use Windows Firewall with Advanced Security to create and enable firewall and connection security rules. These local rules are then merged with the rules received from Group Policy and applied to the computer's active configuration. The setting described in this section prevents the locally defined rules from merging with the rules that are contained in the deployed GPOs.

Important

Although this setting prevents a local administrator from applying a rule, it also prevents Windows Firewall with Advanced Security from prompting the user about a new program and creating an inbound rule when the user approves. If you enable this setting then you must make sure that every program that requires firewall rules has the correct rules defined in your GPOs.

To confirm that a local administrator can create a conflicting rule

|  |
| --- |
| 1. On CLIENT1, at the administrator command prompt, run ping dc1.  The ping command works, which indicates that CLIENT1 can communicate with DC1.  2. Start the Windows Firewall with Advanced Security snap-in.  3. Under Windows Firewall with Advanced Security, right-click Outbound Rules, and then click New Rule.  4. On the Rule Type page of the New Outbound Rule Wizard, click Custom, and then click Next.  5. On the Program page, select All programs, and then click Next.  6. On the Protocol and Ports page, use the default settings, and then click Next.  7. On the Scope page, use the default settings, and then click Next.  8. On the Action page, use the default settings, and then click Next.  9. On the Profile page, clear the check boxes for Private and Public, but leave Domain selected, and then click Next.  10. On the Name page, enter the name A Test Rule (use an 'A' as the first character to ensure the rule appears at the top of the list), and then click Finish.  This creates a firewall rule that blocks all network traffic, effectively breaking communications for the computer.  11. Return to the Command Prompt window, and run ping dc1 again.  The ping command fails, as shown in the lower half of the following figure, because the local firewall rule blocks outgoing communications.    12. In the Windows Firewall with Advanced Security snap-in, click Outbound Rules in the navigation pane, right-click A Test Rule, and then click Disable Rule. You must disable the rule to re-enable communication for the next steps.  13. Leave the Administrator: Command Prompt window and Windows Firewall with Advanced Security snap-in open. |

In the next procedure, you modify the GPO assigned to the client computer to prevent locally defined rules from being merged and applied to the active firewall configuration. Also, you disable the notification that asks the user whether to allow a program for which there are no rules.

To prevent the computer from using rules and settings defined by local administrators

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management, click Group Policy Objects, right-click Firewall Settings for Windows Clients, and then click Edit.  2. In Group Policy Management Editor, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, and then expand Windows Firewall with Advanced Security.  3. Right-click Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com, and then click Properties.  4. On the Domain Profile tab, in the Settings section, click Customize.  5. Change the Display a notification setting to No. This prevents Windows from displaying a notification to the user whenever a program is blocked.  6. In the Rule merging section, change the Apply local firewall rules list to No.  7. In the Rule merging section, change the Apply local connection security rules list to No.  8. Click OK two times to return to Group Policy Management Editor. |

In the next step, you refresh Group Policy on CLIENT1, and then confirm that locally defined rules cannot block network communications.

To test your new restrictions on local administrators

|  |
| --- |
| 1. On CLIENT1, in Administrator: Command Prompt, run gpupdate /force. Wait until the command finishes.  2. In the Windows Firewall with Advanced Security snap-in, in the list of Outbound Rules, right-click A Test Rule, and then click Enable Rule.  3. In Administrator: Command Prompt, run ping dc1.  The ping command works even though A Test Rule appears to be enabled. The rule is listed as enabled on the local computer, but when you set the Apply local firewall rules to No on the GPO in the previous procedure, you blocked the merging of local rules with the rules delivered in the GPO.  4. In the navigation pane of the Windows Firewall with Advanced Security snap-in, expand Monitoring, and then click Firewall to see the list of rules active on the local computer.  No rules are listed. You have not yet created any rules applied by GPO, and no local rules are active because of the settings that you included in the GPO.  5. Before proceeding, delete your rule. On CLIENT1, in the navigation pane, click Outbound Rules. In the results pane, right-click A Test Rule, click Delete, and then click Yes on the confirmation dialog box.  6. Leave both Administrator: Command Prompt and the Windows Firewall with Advanced Security snap-in open. |

Next step: [Step 6: Configuring the Rest of Your Client Computer Firewall Settings](#z1bf9b554d6194b1ea26dc5e891b9ede1)

Step 6: Configuring the Rest of Your Client Computer Firewall Settings

At this point, you have the firewall enabled, and a local administrator cannot disable it. In this step, you complete the configuration of the client computer GPO by adding other frequently used settings to further control the behavior of the firewall on a computer that is running either Windows 7 or Windows Vista.

Any settings in the GPO that you leave on the default value of "Not configured" can be configured by a local administrator. Therefore, you might not want to depend on the default settings. Instead, you should explicitly set those values that you want configured a certain way. The procedures in this section illustrate how to configure other common settings that you typically do not want a local administrator to be able to change.

To see that a local administrator can modify settings that are not enforced by a GPO

|  |
| --- |
| 1. On CLIENT1, in the Windows Firewall with Advanced Security snap-in, in the navigation pane, right-click the top node Windows Firewall with Advanced Security, and then click Properties.  2. On the Domain Profile tab, change Outbound connections to Block, and then click OK.  3. In Administrator: Command Prompt, type ping dc1, and then press ENTER.  Notice that the command fails, because all outgoing network traffic is blocked by Windows Firewall with Advanced Security.  4. In the Windows Firewall with Advanced Security snap-in, right-click the top Windows Firewall with Advanced Security node, and then click Properties.  5. Change Outbound connections back to Allow (default) to restore ordinary operation, and then click OK. |

In the next procedure, you configure the settings in Group Policy so that a local administrator cannot change or disable them.

To configure other common firewall settings in Group Policy

|  |
| --- |
| 1. On MBRSVR1, in the Group Policy Management Editor, right-click Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com, and then click Properties.  2. On the Domain Profile tab, in the State section, set Inbound connections to Block (default), and set Outbound connections to Allow (default). This is, of course, the same behavior to which the client is already set, but setting it in the GPO prevents local administrators from changing the settings.  3. Click OK to save your settings and return to the Group Policy Management Editor. |

In the next procedure, you refresh Group Policy on the client, and confirm that locally defined rules and settings cannot block network communications.

To test your new restrictions on local administrators

|  |
| --- |
| 1. On CLIENT1, in Administrator: Command Prompt, type gpupdate /force, and then press ENTER. Wait until the command finishes.  2. In the navigation pane of the Windows Firewall with Advanced Security snap-in, right-click the top Windows Firewall with Advanced Security node, and then click Properties.  3. On the Domain Profile tab, notice that the restrictions now prevent a local user, even an administrator, from modifying the settings.  Note  The Inbound connection setting still enables you to select Block all connections. This is a security feature to support a quick mitigation of a malware threat, and cannot be blocked by Group Policy.  4. In the Settings section, click Customize, and then notice that the settings that you configured in Group Policy cannot be locally changed.  5. Click Cancel two times to return to the Windows Firewall with Advanced Security snap-in.  6. Close the Windows Firewall with Advanced Security snap-in. |

Next topic: [Step 7: Creating WMI and Group Filters](#z683088705d17423abcb5aa1108933cdf)

Step 7: Creating WMI and Group Filters

When the network includes client computers that run a variety of Windows operating systems, two computers in the same OU might require different settings to achieve the same configuration. For example, a computer that is running Windows XP might require a different setting than a computer that is running Windows 7 or Windows Vista. Two GPOs would be required in that case, one to apply to computers that are running Windows XP, and one to apply to computers that are running the later versions of Windows.

There are also times when you cannot rearrange the computers in your AD OU hierarchy to let you link a GPO to OUs that contain only the computers to which you want the GPO to apply. So Group Policy also supports using access control lists (ACLs) to prevent the GPO from applying to any computer or user account that is not granted permissions to the GPO.

There are two frequently used techniques used to make sure that GPOs only apply to the correct computers:

 Add a Windows Management Instrumentation (WMI) filter to the GPO. A WMI filter enables you to specify criteria that must be matched before the linked GPO is applied to a computer. By letting you filter the computers to which the GPO applies, this reduces the need to further subdivide your OUs in Active Directory. This technique is dynamic, in that the filter is evaluated when the computer attempts to apply the policy. So if you are filtering based on the version of Windows then upgrading the computer from Windows XP to Windows 7 requires no changes to your GPO, because the filter will automatically recognize the change and filter the computer’s access to the GPO accordingly.

 Grant or deny the Apply Policy security permission in the ACL for the GPO. If you put your computers in security groups, you can then grant the Apply Policy permission to only the groups that should use the GPO.

This guide demonstrates both techniques used together. They can also be used individually. Select the filtering types and query parameters based on the needs of your organization. Each enables you to include computers from across organizational units in the Active Directory hierarchy structure.

Important

Windows XP and Windows Server 2003 use different tools and produce different firewall and IPsec settings than the Windows Firewall with Advanced Security tool included with Windows Vista and later versions of Windows. Mixing the settings together on the same computer can cause unexpected connectivity problems that are very difficult to troubleshoot. We recommend that you use the Windows Firewall with Advanced Security snap-in for settings to create the GPOs for computers that are running Windows Vista or later versions of Windows, and use the tools provided in Windows XP or Windows Server 2003 to create the GPOs intended for those operating systems. The techniques demonstrated in this topic are effective at preventing GPOs designed for one version of Windows from applying to another.

In the next procedure, you apply and test a WMI filter that restricts a GPO to applying only to computers that are running Windows Vista or later (including Windows 7). The filter prevents the GPO from applying to any earlier version of Windows, or to a computer that is running any server version of Windows.

To create the WMI filter

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. On MBRSVR1, switch to Group Policy Management.  2. In the navigation pane, right-click WMI Filters, and then click New.  3. In the Name box, type Apply only to Windows Vista or Later.  4. Click Add.  5. In the Query box type:  select \* from Win32\_OperatingSystem where Version like "6.%" and ProductType = "1"  This query filters on both the product version number and the product type.   The Version property returns values that begin with the following characters (the % symbol is a wildcard character that represents other characters that can follow, but do not help distinguish the version number):   |  |  | | --- | --- | | Windows Server 2008 R2 or Windows 7 | 6.1% | | Windows Server 2008 or Windows Vista | 6.0% | | Windows Server 2003 | 5.2% | | Windows XP | 5.1% | | Windows 2000 | 5.0% |    The ProductType property returns the following values:   |  |  | | --- | --- | | Client versions of Windows | 1 | | Server versions of Windows that are operating as a domain controller | 2 | | Server versions of Windows that are not operating as a domain controller (typically referred to as member servers) | 3 |   6. Click OK, and then click Save.  7. Under Group Policy Objects, click Firewall Settings for Windows Clients.  8. Click the Scope tab, and under WMI Filtering, select your filter Apply Only to Windows Vista or Later from the list.  9. In the confirmation dialog box, click Yes.  The policy now only applies to computers that are running a Windows operating system reporting a version number that starts with the character "6." and that reports that it is a client version of Windows.  10. Leave the Group Policy Management MMC snap-in running. |

In the next procedure, you deploy the policy to see that it does apply to the client computer that is running Windows 7 or Windows Vista.

To deploy and test your WMI filter

|  |
| --- |
| 1. On CLIENT1, in Administrator: Command Prompt, run gpupdate /force. Wait for the command to finish.  2. At the command prompt, type the command gpresult /r /scope computer and confirm that the Applied Group Policy Objects section still contains Firewall Settings for Windows Clients.  3. Leave Administrator: Command Prompt open. |

In the next several procedures, you test group filtering with security ACLs. When combined with the techniques in the previous sections, this results in a GPO that applies only to the members of a group that also meet the requirements of the WMI filter.

To create the computer group

|  |
| --- |
| 1. On DC1, if the Active Directory Users and Computers snap-in is not open, open it. Click click Start, click Administrative Tools, and then click Active Directory Users and Computers.  2. In the navigation pane, right-click Computers, click New, and then click Group.  3. In Group name, type Windows Client Computers, and then click OK. |

In the next procedure, you set the permissions on the GPO to grant the apply policy permission only to members of your new computer group.

To set ACL permissions on the GPO

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management, expand Group Policy Objects, and then click Firewall Settings for Windows Clients.  2. On the Scope tab, in the Security Filtering section, click Authenticated Users, and then click Remove.  3. On the confirmation dialog box, click OK.  4. Click Add, type Windows Client Computers, and then click OK. |

Your computer is not yet a member of this new group. Verify that the GPO does not apply.

To verify that the GPO no longer applies to CLIENT1

|  |
| --- |
| 1. On CLIENT1, open an Administrator: Command Prompt, and then run gpupdate /force. Wait for the command to finish.  2. Type gpresult /r /scope computer. Examine the Applied Group Policy Objects section and verify that the only GPO listed is Default Domain Policy.  3. Look down several more lines under The following GPOs were not applied because they were filtered out and confirm that Firewall Settings for Windows Clients is now listed there.  4. If it is still open, close the Windows Firewall with Advanced Security snap-in, and then restart it.  5. In the navigation pane, right-click Windows Firewall with Advanced Security on Local Computer, and then click Properties.  6. Confirm that all the controls are enabled again because the GPO no longer applies.  7. Click Cancel to close the Properties page. |

In the next procedure, you add the computer to the new group.

To add CLIENT1 to the group

|  |
| --- |
| 1. On DC1, in the Active Directory Users and Computers snap-in, select the Computers container, and then double-click Windows Client Computers in the results pane.  2. Select the Members tab, and then click Add.  3. Click Object Types.  4. Clear all check boxes except Computers, and then click OK.  5. In the text box, type CLIENT1, and then click OK to save your changes. |

Finally, you can apply the GPO to your computer to see the results.

To apply the GPO applied to the computer

|  |
| --- |
| 1. On CLIENT1, restart the computer. The changes to the group membership must be refreshed in the local computer's security tokens. This occurs when the computer starts.  2. Log on as contoso/admin1.  3. Open an Administrator: Command Prompt, and run gpresult /r /scope computer.  4. Examine the output to confirm that the GPO is applied to your computer again.  5. Open the Windows Firewall with Advanced Security snap-in.  6. In the navigation pane, right-click Windows Firewall with Advanced Security on Local Computer, and then click Properties.  7. Confirm that some of the controls are disabled again because they are now controlled by Group Policy.  8. Click Cancel to close the Properties page. |

For more information about how to use WMI filters and Group Policy, see:

 [HOWTO: Leverage Group Policies with WMI Filters](http://go.microsoft.com/fwlink/?linkid=93760) at http://go.microsoft.com/fwlink/?linkid=93760

 [Windows Server Group Policy](http://go.microsoft.com/fwlink/?linkid=93542) at http://go.microsoft.com/fwlink/?linkid=93542

Next topic: [Step 8: Enabling Firewall Logging](#z6c16ece5dfd84ac09deb93080294e38f)

Step 8: Enabling Firewall Logging

When you create or modify firewall rules, you can sometimes end up with a rule set that allows traffic that you do not want, or that blocks traffic that you require. To help troubleshoot these types of problems, Windows Firewall with Advanced Security provides several different ways to capture details about the failure to help you diagnose the connection.

Windows Firewall with Advanced Security in Windows 7 and Windows Server 2008 R2 support the following logging/tracing tools:

 The firewall log file that records allowed or dropped network packets as configured by the firewall Group Policy settings.

 The Windows Firewall with Advanced Security operational event logs that can be viewed in Event Viewer. The events in this log show the operational status of Windows Firewall with Advanced Security and changes in its configuration.

 As in Windows Vista, Windows 7 continues to support audit events that can track certain symptoms and errors in Windows Firewall with Advanced Security. Audit events must be enabled before they appear in the Event Viewer.

 The netsh wfp capture command that captures detailed diagnostic information about networking operations on the computer during the capture session.

 The nesh trace commands to enable network tracing with filters that capture network traffic relevant to a selected scenario. The WFP-IPsec scenario, for example, captures information specifically related to the operation of the Windows Filtering Platform (WFP) and IPsec.

Each of these is introduced in the next several procedures.

First, you configure your server GPO to create a local file that logs both allowed packets and dropped packets. Later in this guide, after you create and test some firewall rules, you examine this log file to see the kinds of entries created there.

To configure a firewall log file in your server GPO

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management, in the navigation pane, right-click Firewall Settings for Windows Servers, and then click Edit. Be sure to open the SERVER GPO, not the client one.  2. In the Group Policy Management Editor, right-click the top node in the navigation pane, and then click Properties.  3. Select the Disable User Configuration settings check box.  4. In the confirmation dialog box, click Yes, and then click OK.  5. In the navigation pane, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, and then expand Windows Firewall with Advanced Security.  6. Right-click Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com, and then click Properties.  7. On the Domain Profile tab, in the Logging section, click Customize.  8. Clear both Not configured check boxes. You can use the default values for path and maximum size.  9. Change Log dropped packets to Yes.  10. Change Log successful connections to Yes.  11. Click OK two times to save your GPO.  12. Close the Group Policy Management Editor. |

To apply this GPO to the correct set of computers, link the GPO to the OU.

Note

For simplicity, you do not create a WMI filter or security group as you did with the client GPO, but the exact same principles could be applied here to filter the GPO only to member servers in the domain that are running Windows Server 2008 or Windows Server 2008 R2.

To deploy and test your server GPO

|  |
| --- |
| 1. On MBRSVR1, in the Group Policy Management console, right-click the OU MyMemberServers that you created earlier, and then click Link an Existing GPO.  2. In the Select GPO dialog box, select Firewall Settings for Windows Servers, and then click OK.  3. Still on MBRSVR1, in the Administrator: Command Prompt, run gpupdate /force. Wait for the command to finish.  4. Open the Windows Firewall with Advanced Security snap-in.  5. In the navigation pane, right-click Windows Firewall with Advanced Security on Local Computer, and then click Properties.  6. On the Domain Profile tab, in the Logging section, click Customize.  7. Confirm that the settings in your GPO now appear as the active settings for this computer.  8. Click OK two times to close the dialog boxes.  9. Leave Administrator: Command Prompt and the Windows Firewall with Advanced Security snap-in open. |

Windows also writes operational events to the event log that is viewable by using Event Viewer. In earlier versions of Windows, most information of interest to an administrator was found in the System and Application logs. Starting with Windows Vista and later versions of Windows, the Event Viewer includes many predefined filtered views. The original, unfiltered System and Application logs can be found under Windows Logs . The filtered list of Windows Firewall with Advanced Security events can be found under Application and Services Logs, Microsoft, Windows, Windows Firewall with Advanced Security.

To examine the Firewall Operational Event Logs

|  |
| --- |
| 1. On MBRSVR1, click Start, click Administrative Tools, and then click Event Viewer.  2. In the navigation pane, expand Applications and Service Logs, expand Microsoft, expand Windows, and then expand Windows Firewall with Advanced Security.  3. Examine the four categories under the Windows Firewall with Advanced Security node. The two main functions of Windows Firewall with Advanced Security, IPsec and host-based Firewall have their events stored under the ConnectionSecurity and Firewall nodes, respectively. The ConnectionSecurityVerbose and FirewallVerbose nodes are disabled by default.  4. In the navigation pane, select the Firewall node.  There are a variety of events already present. These events document configuration changes to the operational state of the firewall. Among the events should be those with Event IDs 2002, 2003, 2004, 2008, 2010, 2011, and 2012. If you open Event Viewer on CLIENT1, you will also see Event IDs 2005, and 2006 that document modifying and then deleting the rule “A Test Rule”.  5. Select the topmost event with an Event ID number of 2003. If you followed the steps in this guide, this event is the changing of Log File Path setting in the Domain profile, caused by applying your modified member server GPO.  6. To enable the verbose logs, right-click ConnectionSecurityVerbose and FirewallVerbose, and then click Enable log. |

Windows 7 and Windows Server 2008 R2 introduce the new netsh wfp context that enables you to capture diagnostic trace sessions of the behavior of the Windows Filtering Platform which is the base engine that implements your firewall and connection security rules. Starting a capture session, reproducing the problem, and then stopping the capture results in a log that can help you or Microsoft Customer Support Services (CSS) troubleshoot connectivity problems on your computers.

To capture a Netsh WFP diagnostics session

|  |
| --- |
| 1. On MBRSVR1, open and administrative command prompt.  2. At the command prompt, change the current folder to your desktop by running the command: cd %userprofile%\desktop  3. To start the capture, run the command netsh wfp capture start.  4. At this point in a real troubleshooting situation, you would reproduce the problem. For our purposes, just wait a few seconds.  5. To complete the capture, run the command netsh wfp capture stop. The output file is stored in the current folder.  6. Double-click the .cab file that is on the desktop.  7. The .cab file contains an .xml file and an .etl file. The .etl file is a binary file that is intended for use by CSS. The .xml file can be loaded and read locally. Because of the size of the .xml files produced by this process we recommend that you acquire an XML Reader program, instead of using a Web browser or Notepad to open the file.  8. Drag the wfpdiag.xml file to the desktop from the .cab file.  9. Open the file with your XML reader of choice and examine the contents. Note the main sections:   sysInfo – This section contains information about the computer on which the trace was captured.   initialState – This section contains information about the state of the WFP and the currently configured rules before the problem was reproduced.   Events – This section contains information about things that occurred while the capture session was running.   finalState – This section contains the same information as initialState, but was captured when you ran the wfp capture stop command. You can directly compare the two sections to look for differences that might relate to the connection problem you are trying to diagnose. |

Similarly, you can use the netsh trace and netsh trace stop commands to capture a variety of diagnostic information customized to a selected scenario, such as wfp-ipsec.

By using one or more of the logging techniques demonstrated earlier in this section, you can learn much about why a particular connection does or does not work.

To capture a Netsh Trace diagnostics section

|  |
| --- |
| 1. At an Administrator: Command Prompt, run the command netsh trace start scenario=wfp-ipsec tracefile=%userprofile%\desktop\SampleTrace.cab  The output of the command shows you that the trace is running, the file to which the data is written, and details of other possible parameters.  2. In a production troubleshooting environment, this is where you would attempt to reproduce the problem.  3. In this sample, after a few seconds, run the command netsh trace stop.  The computer takes a few moments to compile the collected trace data into a .cab file at your specified location.  4. On the desktop, double-click sampletrace, and examine its contents. A variety of text files, .xml files, event log files, and other types are included. Double-click some of them to view their contents.  5. When you have finished examining the files, close the .cab file, and the command prompt. |

Next topic: [Creating Rules that Allow Required Inbound Network Traffic](#ze5c2f8ea3b1d44df8307ea5bfa96b7e0)

Creating Rules that Allow Required Inbound Network Traffic

By default, Windows Firewall with Advanced Security blocks all unsolicited inbound network traffic. To enable programs that depend on such traffic to run correctly, such as network services, you must create rules with specified criteria.

Note

One of the most important improvements in Windows Vista and Windows 7, enabled by the integration of IPsec and the Windows Firewall, is the ability to create inbound firewall rules that only allow traffic that is authenticated, optionally encrypted, or authorized by the requesting user or computer being a member of an allowed group. These advanced inbound rule types are discussed as part of the [server isolation scenario found later in this guide](#zfb995b0bce8b4507a6531acdf5ef8ff5). Also, when network traffic is protected by IPsec and meets your criteria, you can choose to configure an inbound rule to override a block rule that would otherwise have blocked the network traffic. This scenario is discussed in the [authenticated bypass scenario found later in this guide](#zd9891d8917d74cf3a08de4a46904a7a2).

Steps for creating rules that allow required inbound network traffic

In this section of the guide, you create firewall rules that allow specific types of unsolicited inbound network traffic through the firewall.

[Step 1: Configuring Predefined Rules by Using Group Policy](#z1823b7a824fb451d83b523b912118884)

[Step 2: Allowing Unsolicited Inbound Network Traffic for a Specific Program](#zc3bb5b29b6a84fd4a66dddb39767b2ea)

[Step 3: Allowing Inbound Traffic to a Specified TCP or UDP Port](#z5de9930128104616b6f9a1d27b377e7c)

[Step 4: Allowing Inbound Network Traffic that Uses Dynamic RPC](#zd37f96c6c7294b2980a988db3d97b863)

[Step 5: Viewing the Firewall Log](#z471fe7212f2c4e438693c25d59f020cd)

Next topic: [Step 1: Configuring Predefined Rules by Using Group Policy](#z1823b7a824fb451d83b523b912118884)

Step 1: Configuring Predefined Rules by Using Group Policy

In many scenarios, you might want to configure rules that allow generally required network activity, such as certain ICMP response types, which are not associated with a service, but are required for some network troubleshooting. The most common network traffic types required by both clients and servers are specified in Windows Firewall with Advanced Security by predefined sets of rules. This makes it easy to select them for configuration and deployment. This guide only demonstrates with one predefine group. In a production environment, examine all of the provided predefined groups and deploy those that are appropriate for your organization’s network.

In this step, you use the Group Policy Management MMC snap-in to configure a group of firewall rules. You set the rules that are part of the group Core Networking to be always enabled.

To configure a group of firewall rules

|  |
| --- |
| 1. On MBRSVR1, in the Group Policy Management snap-in, right-click Firewall Settings for Windows Clients, and then click Edit.  2. In the navigation pane of the Group Policy Management Editor, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Windows Firewall with Advanced Security, and then expand Windows Firewall with Advanced Security - LDAP://{GUID},cn=policies,cn=system,DC=contoso,DC=com.  3. Click Inbound Rules.  There are no inbound firewall rules in the GPO by default.  4. Right-click Inbound Rules, and then click New rule.  5. On the Rule Type page of the wizard, click Predefined, select Core Networking from the list, and then click Next.  6. On the Predefined Rules page, examine the list of rules, leave them all selected, and then click Next.  Note  In a production environment, carefully consider which profiles you apply the rules to. You may want to consider rules for other profiles to control how the firewall works on computers that are away from the network, such as portable computers which are taken home. You might want to consider applying your rules to all the profiles to make sure that your organization's computers continue to be protected when they are away from the organization's network. Some rule modifications may be required to allow expected program behavior on a home or public network that differs from the organization's network.  7. On the Action page, because we want to create an exception for traffic that would by default be blocked, select Allow the connection, and then click Finish.  The list of enabled rules now appears in the results pane for Inbound Rules.    8. Close the Group Policy Management Editor for the client GPO. |

With the list of rules now in the GPO, deploy the GPO to the client computer.

To test the rules on the client computer

|  |
| --- |
| 1. On CLIENT1, in Administrator: Command Prompt, run gpupdate /force. Wait until the command finishes.  2. In the navigation pane of the Windows Firewall with Advanced Security snap-in, expand Monitoring, and then click Firewall.  Note the list of rules that is now active on the local computer. It may take several seconds for the list to populate.  3. Click View, and then click Add/Remove columns.  4. If the Rule Source column is not displayed, click Rule Source in the Available columns list, and then click Add.  5. Click Move Up to position Rule Source directly after Name, and then click OK.  6. Note that all the rules identify the GPO Firewall Settings for Windows Clients as the source of the rule. Even if you disable the locally defined Core Networking rules under Inbound Rules, these rules from the GPO still apply to the computer. |

Next topic: [Step 2: Allowing Unsolicited Inbound Network Traffic for a Specific Program](#zc3bb5b29b6a84fd4a66dddb39767b2ea)

Step 2: Allowing Unsolicited Inbound Network Traffic for a Specific Program

When you use a program that must be able to receive unsolicited inbound network traffic, you must create a rule to permit that traffic to pass through the firewall. Client computers typically do not need this, because incoming network packets are responses to previous outgoing requests to servers elsewhere on the network. However, if you install a network service then your computer will receive unsolicited network traffic from clients to the service. Servers, of course, also expect unsolicited inbound network traffic for the services hosted on them.

By default on Windows 7 and Windows Vista, when you start such a program and it registers with Windows to listen on a specific TCP or UDP port number, Windows blocks the request and displays a dialog box asking for your instructions. If you decide to allow the program then Windows automatically creates a firewall rule to allow all network traffic for that program. You can also create a similar rule manually. If you create such a rule and distribute it by using Group Policy then users do not have to see the dialog box and decide what to do.

By default on computers that are running Windows Server 2008 R2 or Windows Server 2008, the notification dialog box does not appear, but the program is still silently blocked. If firewall logging of dropped packets is enabled, as you did in the last section then the log file is the only indication that these packets arrived and were dropped. So on computers that are running one of those versions of Windows Server, you must create rules for each program or service that requires unsolicited inbound network traffic. Another advantage to creating the rule manually is that you can customize the rule to restrict it to only the specific traffic required by the program.

Note

While not demonstrated in this guide, there is another option of which you should be aware. The IPv6 transition technology called Teredo involves tunneling IPv6 packets inside IPv4 packets with UDP headers. Because UDP can be translated by a network address translator (NAT), Teredo enables IPv6 clients to communicate even if the clients are behind one or more IPv4 NATs. To correctly process this kind of IPv6 embedded in IPv4 traffic, firewall rules support an “edge traversal” option. If your firewall rule is for a client computer that might be receiving inbound traffic from a remote computer over a Teredo tunnel then the firewall rule must specify Allow edge traversal. On the firewall rule Properties page, on the Advanced tab, under Edge traversal, select Allow edge traversal. For more information about Teredo, see [Teredo Overview](http://go.microsoft.com/fwlink/?linkid=159757) (http://go.microsoft.com/fwlink/?linkid=159757) in the Windows Server Technical Library.

In this section, as a first example, you create a firewall rule that allows inbound traffic for the Telnet service through the firewall, and then you deploy that rule to MBRSVR1 by using Group Policy.

To create a firewall rule that allows inbound traffic for a program

|  |
| --- |
| 1. On MBRSVR1, in the Group Policy Management window, right-click Firewall Settings for Windows Servers (not clients), and then click Edit.  2. In the navigation pane, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Windows Firewall with Advanced Security, and then expand Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,dc=com.  3. Right-click Inbound Rules, and then click New rule.  4. On the Rule Type page, click Custom, and then click Next.  Note  We recommend that you create rules that are as specific as possible. That means you might want to specify both the program, to ensure the rule only allows traffic when that program is running, and the port, to make sure that the program can only receive on the specified port number. To see all the options available in the wizard, use the Custom rule type.  5. In the text box for This program path, type %systemroot%\system32\tlntsvr.exe.  6. Because programs can host multiple services, we recommend that you also limit the rule to the specific service you want. Next to Services, click Customize.  7. Click Apply to this service, select Telnet, click OK, and then click Next.  Note  The list of services includes only the services currently installed on the computer on which you are editing the GPO. If the service you want to specify is not installed on this computer, you can use the option Apply to service with this service short name, and then type the service name in the text box. To discover the service short name, use the Services MMC snap-in on a computer on which the service is installed.  8. On the Protocols and Ports page, click Next. You restrict the rule to a specific port in the next section.  9. On the Scope page, click Next.  10. On the Action page, select Allow the Connection, and then click Next.  11. On the Profile page, clear the Private and Public check boxes. Confirm that Domain is selected, and then click Next.  12. On the Name page, type Allow Inbound Telnet, and then click Finish. |

Before you deploy the GPO, configure some other settings to make sure that locally defined rules on your server computers cannot interfere with your domain provided rules.

To finish configuring the firewall rule for the member server

|  |
| --- |
| 1. In the navigation pane of the Group Policy Management Editor (editing Firewall Settings for Windows Servers), right-click Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,dc=com, and then click Properties.  2. Set Firewall state to On (recommended).  3. Set Inbound connections to Block (default).  4. Set Outbound connections to Allow (default). You will examine outbound rules in the next section.  5. In the Settings section, click Customize.  6. Set Display a notification to No.  7. Set Apply local firewall rules to No.  8. Set Apply local connection security rules to No.  9. Click OK two times to save your GPO. |

In this procedure, you deploy your GPO to your member server.

To update the GPO on the member server

|  |
| --- |
| 1. Open Administrator: Command Prompt, and then run gpupdate /force. Wait for the command to finish.  2. Open the Windows Firewall with Advanced Security snap-in.  3. In the navigation pane, expand Monitoring, and then click Firewall. Note that the only currently active rule is the Allow Inbound Telnet rule that you created in the GPO. |

In this procedure, you test the deployed firewall rule.

To test the Telnet firewall rule

|  |
| --- |
| 1. On CLIENT1, at Administrator: Command Prompt, type telnet mbrsvr1, and then press ENTER.  After several seconds the following screen appears and indicates that your Telnet firewall rule is working.    2. Close the Telnet session by typing exit, and then pressing ENTER. |

In this procedure, you confirm that it is not the local Telnet rule that was created when the Telnet Server service was installed on MBRSVR1. You disable that rule and confirm that Telnet still works because your GPO applied rule is active.

To confirm that it is your GPO rule that allows Telnet to work

|  |
| --- |
| 1. On MBRSVR1, in the Windows Firewall with Advanced Security snap-in, in the navigation pane, click Inbound Rules. Note your GPO-based Telnet firewall rule is listed at the top.  2. Scroll down to the rule named Telnet Server, right-click it, and then click Disable rule.  3. On CLIENT1, at the command prompt, run telnet mbrsvr1 again, and then confirm that it is still working.  4. Close the Telnet session by typing exit, and then pressing ENTER. |

Finally, you demonstrate that the Telnet service can listen for network traffic on any port the way the rule is currently configured.

To show that the firewall rule allows Telnet network traffic on a specified port

|  |
| --- |
| 1. On MBRSVR1, at an Administrator: Command Prompt, type tlntadmn config port=25, and then press ENTER. This configures your Telnet server to listen on port 25 instead of the default port 23.  2. On CLIENT1, at a command prompt, type telnet mbrsvr1 25. This instructs the client to use port 25 for its connection instead of the default port 23.  The connection succeeds. |

In the next section, you configure the rule to allow traffic only on a port number you specify. This is an improvement in security, because it allows traffic only on those ports on which you have active services listening.

Next topic: [Step 3: Allowing Inbound Traffic to a Specified TCP or UDP Port](#z5de9930128104616b6f9a1d27b377e7c)

Step 3: Allowing Inbound Traffic to a Specified TCP or UDP Port

In the previous step, you created a rule that allows unsolicited inbound network traffic only to the Telnet Server service. However, it is considered a best practice to also limit the traffic to only those TCP or UDP ports that the service actually uses. In the case of a standard Telnet deployment, only TCP port 23 is required.

In this procedure, you refine the Telnet exception rule to limit the allowed inbound network traffic to TCP port 23 only.

To configure the rule to limit traffic to a specific port

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management Editor for your server GPO, click Inbound Rules.  2. In the results pane, right-click Allow Inbound Telnet, and then click Properties.  3. Click the Protocols and Ports tab.  4. In Protocol type, click TCP. Note that the Protocol number automatically changes to 6.  5. In the Local port list, click Specific Ports.  6. In the text box directly under Local Port, type 23.  7. Click OK to save your changes. |

In this procedure, you test the modified rule.

To test your modified rule

|  |
| --- |
| 1. On MBRSVR1, at Administrator: Command Prompt, run gpupdate /force. Wait until the command finishes.  Because the Telnet service on MBRSVR1 is still configured to listen on port 25, the service should not be able to receive any traffic.  2. On CLIENT1, at a command prompt, run telnet mbrsvr1 25.  The command times out and fails because the firewall on MBRSVR1 now blocks all inbound traffic to the Telnet service except port 23.  3. On MBRSVR1, at the Administrator: Command Prompt, run tlntadmn config port=23 to restore the service to the default port number.  4. On CLIENT1, at the command prompt, run telnet mbrsvr1.  The command succeeds because the firewall allows inbound network traffic to port 23 to the Telnet service which is configured to listen on that port.  5. Close the Telnet session by typing exit, and then pressing ENTER. |

Next topic: [Step 4: Allowing Inbound Network Traffic that Uses Dynamic RPC](#zd37f96c6c7294b2980a988db3d97b863)

Step 4: Allowing Inbound Network Traffic that Uses Dynamic RPC

If every program and service that needed to communicate over the network assigned its own port number, you can easily imagine that sooner or later two programs would conflict over the use of the same port. To address this, many programs use the Remote Procedure Call (RPC) protocol to request communications with a host service on a dynamically assigned port number. When a service starts up, it registers with the RPC service and requests the assignment of one or more dynamic port numbers. When the remote client needs to communicate with that service, it does not know which port numbers have been assigned. To find out, the client connects to the server on TCP port 135 (the "well-known" port number for the RPC Endpoint Mapper service), and identifies the service to which it wants to connect. The RPC Endpoint Mapper service replies with the port number that the client should use to connect to the desired service. The client then reconnects to the server using the assigned port number, and communication with the desired service begins.

In versions of Windows earlier than Windows Vista, dynamically assigned ports have been a challenge for firewall administrators. Either they had to create rules that open large ranges of port numbers in the dynamically assigned range (all ports greater than 1024), or they had to limit the program to using a much smaller number of ports than it was designed to use. Creating rules to open many ports that are not currently being actively used increases the surface area of a computer's vulnerability to attack. Limiting programs to using fewer ports might compromise the programs' performance, and some programs provide no way to configure or limit the port numbers used. Neither is a good situation.

Starting in Windows Vista, Windows Firewall with Advanced Security supports stateful filtering of the dynamically assigned port numbers used by RPC. Only those port numbers currently assigned by RPC to an active service are opened, and even then, a dynamically assigned port is opened only to clients that asked to connect to that service by making a request to the RPC Endpoint Mapper.

Note

To determine whether your program must use ports that are dynamically assigned by RPC, see the documentation provided by your program's vendor. You can also examine the traffic going to and from your program by using a network protocol analyzer such as Microsoft Network Monitor. You can download Network Monitor at <http://go.microsoft.com/fwlink/?LinkID=94770>. See the Network Monitor Links section in the left-hand column

In Windows Vista and later versions of Windows, this problem is solved by the introduction of rules that can directly support RPC port requirements for programs. To configure this support for a program, you must create the following rules:

 An inbound rule that allows inbound network traffic for RPC Endpoint Mapper. This rule allows the computer to receive traffic sent to the port 135. The rule must also be configured to use the Allow action, and the program path of the RPC Endpoint Mapper service.

 An inbound rule that specifies Dynamic RPC for the port number. When an incoming request from a remote computer is received by the RPC Endpoint Mapper service on port 135 (see the previous rule), the service assigns a dynamic port number to the request and replies to the remote computer by using that number. The IP address of the remote computer and the dynamic port number are stored in an internal table. When the remote computer then sends a packet to the new port number, this rule allows Windows to match the port number and IP address to the entries stored in the table. If a match is found, it allows the inbound traffic.

The advantage is that any port in the RPC ephemeral range can be used without having to explicitly define a rule to open that port. The port is only usable by a program that was assigned the use of the port by the endpoint mapper. No unused ports are left open, reducing the vulnerability of the server.

Important

If you create rules to allow RPC network traffic through the firewall then all RPC network traffic is permitted. Windows Firewall cannot filter network traffic based on the UUID of the destination program.

In this section, you create rules for the Remote Event Log service that use Dynamic RPC. Although Windows has predefined rules that provide this capability, you create the rules manually to see the steps that are involved.

To begin, confirm that the Remote Event Log service is not currently working remotely from the client because the firewall on MBRSVR1 is blocking the traffic.

To confirm that the Remote Event Log service is not working remotely

|  |
| --- |
| 1. On CLIENT1, click Start, type event viewer in the Start Search box, and then press ENTER.  2. Click Action, and then click Connect to another computer.  3. In the Another computer text box, type MBRSVR1, and then click OK.  4. After several seconds, the connection attempt times out and fails as shown in the following figure, because Windows Firewall with Advanced Security on MBRSVR1 is dropping the required network traffic. Click OK. |

To allow this service to work, begin by creating a rule that supports inbound traffic to the RPC Endpoint Mapper service. This example shows how to create a firewall rule that restricts a services container (svchost.exe) that hosts many services to only the one service of interest, and then further restricts that service to only the required TCP port.

To create a rule that allows inbound network traffic to the RPC Endpoint Mapper service

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management Editor for your server GPO, in the navigation pane, right-click Inbound Rules, and then click New rule.  2. On the Rule Type page, click Custom, and then click Next.  3. In the This program path text box, type %systemroot%\system32\svchost.exe.  4. Next to Services, click Customize.  5. Click Apply to this service, select Remote Procedure Call (RPC) with a short name of RpcSs, click OK, and then click Next.  6. On the warning about conflicting with Windows service-hardening rules, click Yes.  7. On the Protocol and Ports page, for Protocol type, select TCP.  8. For Local Port, select RPC Endpoint Mapper, and then click Next.  9. On the Scope page, click Next.  10. On the Action page, click Next.  11. On the Profile page, clear the Private and Public check boxes, and then click Next.  12. On the Name page, type Allow RPC Endpoint Mapper, and then click Finish. |

Next, create a rule that allows the incoming traffic from the remote Event Log client. Since the incoming port number is assigned dynamically by the RPC Endpoint Mapper service, you specify Dynamic RPC instead of a specific port number.

Note

The Event Log we are using as an example service is hosted in %systemroot%\system32\svchost.exe. Be sure to use the path of the executable file hosting the service that you want to create rules for when in a production environment.

To create a rule that allows inbound network traffic to your RPC-enabled service

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management Editor, in the navigation pane, right-click Inbound Rules, and then click New rule.  2. On the Rule Type page, click Custom, and then click Next.  3. In the This program path text box, type %systemroot%\system32\svchost.exe. The Remote Event Log service is another service hosted by that file.  4. Next to Services, click Customize.  5. Click Apply to this service, select Windows Event Log with a short name of eventlog, click OK, and then click Next.  6. On the warning about conflicting with Windows service-hardening rules, click Yes.  7. On the Protocol and Ports page, for Protocol type, select TCP.  8. For Local Port, select Dynamic RPC (on Windows Server 2008) or RPC Dynamic Ports (on Windows Server 2008 R2), and then click Next.  9. On the Scope page, click Next.  10. On the Action page, click Next.  11. On the Profile page, clear the Private and Public check boxes, and then click Next.  12. On the Name page, type Allow Remote Event Log Service, and then click Finish.  Now you can apply the GPO to MBRSVR1.  13. At an Administrator: Command Prompt, run gpupdate /force. Wait for the command to finish.  14. If it is not already open, open the Windows Firewall with Advanced Security snap-in.  15. Expand Monitoring, click Firewall, and then confirm that your new rules are now active on the computer. |

Now you can try to connect to the Remote Event Log service from the client again.

To confirm that the Remote Event Log service is working

|  |
| --- |
| 1. On CLIENT1, in Event Viewer, click Action, and then click Connect to another computer.  2. In the Another computer text box, type MBRSVR1, and then click OK.  3. The attempt succeeds, and the top node in the navigation page shows that the viewer is connected to MBRSVR1.contoso.com.    4. Close Event Viewer. |

Next topic: [Step 5: Viewing the Firewall Log](#z471fe7212f2c4e438693c25d59f020cd)

Step 5: Viewing the Firewall Log

You have created several connections to your server after turning on firewall logging, and you also had several connections blocked by the firewall rules you put in place. In this step, you examine the log that accumulated to this point and then you turn the logging back off.

To examine the firewall log

|  |
| --- |
| 1. On MBRSVR1, if it is not already open, open the Windows Firewall with Advanced Security snap-in.  2. In the navigation pane, click Monitoring. In the Details pane, under Logging Settings, click the file path next to File name. The log opens in Notepad.  3. In Notepad, examine the entries. There are many more entries than those related directly to your activity for this guide. There are Domain Name System (DNS) queries, network basic input/output (NetBIOS) protocol connections, and so on.  4. Search for lines that resemble the following examples. You can press CTRL-F to open a search dialog box, and enter a [space] 23 [space]. Be sure to include the spaces, so that you do not find the number 23 embedded in other numbers.  The values in italic in the samples that follow might vary from those in your log. The final column is not shown here, but is often of interest, because it shows whether the packet was an inbound (RECEIVE) or outbound (SEND) packet.   The following entries represent the allowed Telnet connections on ports 23 and 25:  2009-06-09 10:10:48 ALLOW TCP 192.168.0.101 192.168.0.100 52174 23  2009-06-09 10:15:54 ALLOW TCP 192.168.0.101 192.168.0.100 52175 25   The following entry represents a blocked Telnet connection attempt on port 25:  2009-06-09 10:28:28 DROP TCP 192.168.0.101 192.168.0.100 52180 25   The following entries shows the allowed Remote Event Log connection:  2009-06-09 10:49:59 ALLOW TCP 192.168.0.101 192.168.0.100 52191 135  2009-06-09 10:50:00 ALLOW TCP 192.168.0.101 192.168.0.100 52192 49153  5. Close Notepad. |

Note

In production troubleshooting scenarios, you can import your log file into Microsoft Excel to more easily search, sort, and filter the entries. Use the space character as the separator when you import the log file.

You should only turn on logging when you need it, such as when you are troubleshooting. Because we are finished, turn the logging off.

To turn Firewall logging off

|  |
| --- |
| 1. Switch to the Group Policy Management Editor window that is configuring your Server GPO.  2. In the navigation pane, right-click Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com, and then click Properties.  3. On the Domain Profile tab, under Logging, click Customize.  4. Change Log dropped packets to No (default).  5. Change Log successful connections to No (default).  6. Click OK two times to save your changes.  7. At the Administrator: Command Prompt, run gpupdate /force. Wait until the command is finished. |

Next topic: [Creating Rules that Block Unwanted Outbound Network Traffic](#zc0b58af6447e4a47ae46bb68fdeaf203)

Creating Rules that Block Unwanted Outbound Network Traffic

By default, Windows Firewall with Advanced Security allows all outbound network traffic. If your organization prohibits specific network programs on organization computers, you can help enforce that prohibition by blocking the network traffic that the programs require to operate correctly.

By default, inbound network traffic to a computer that does not match a rule is blocked, but nothing prevents outbound traffic from leaving a computer. To block the network traffic for prohibited programs, you must create an outbound rule that blocks traffic with specific criteria from passing through Windows Firewall with Advanced Security. Alternatively, you can change the default outbound action to block, and then create outbound allow rules to allow required traffic. This is the technique demonstrated in this section.

Steps for blocking outbound network traffic and creating rules that allow permitted outbound network traffic

In this section of the guide, you configure the default outbound behavior to block outbound network traffic. You then create a rule that permits outbound Telnet traffic.

[Step 1: Configuring the Default Outbound Firewall Behavior to Block](#z28e43c811013495b9a75984676d3ba11)

[Step 2: Allowing Network Traffic for a Program by Using an Outbound Rule](#zfc608cea6af840a3bc626713162abfb3)

Next topic: [Step 1: Configuring the Default Outbound Firewall Behavior to Block](#z28e43c811013495b9a75984676d3ba11)

Step 1: Configuring the Default Outbound Firewall Behavior to Block

In this step, you change the default outbound behavior for the firewall. By default, Windows Firewall allows all outbound network traffic. In order to restrict outbound traffic, you can change that default to cause Windows Firewall with Advanced Security to block all outbound traffic that does not match an outbound allow rule.

Important

In a production environment, you must carefully evaluate the outbound traffic requirements for your computers. You must then create outbound allow rules for all network traffic that must be permitted. Any additional applications that must be able to transmit on the network must have rules created and deployed. Be sure to test your configuration before you deploy it to production computers.

To configure the default outbound behavior to block

|  |
| --- |
| 1. On MBRSVR1, if Group Policy Management Editor is still open, close it.  2. In Group Policy Management, right-click Firewall Settings for Windows Clients, and then click Edit.  3. Expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Windows Firewall with Advanced Security, and then expand Windows Firewall with Advanced Security - LDAP://{GUID},cn=policies,cn=system,DC=contoso,DC=com.  4. Before you enable the default outbound block, enable the Core Networking and File and Printer Sharing outbound rules that will permit the client to continue to receive changes in Group Policy. Because your settings prevent local rules from being used, you must include them in the GPO. In the navigation page, right-click Outbound Rules, and then click New Rule.  Caution  Be sure to test your rules carefully in a lab environment before you apply them to production computers. If you do not allow the required outbound traffic then the client cannot even talk to the domain controller to retrieve an updated GPO that fixes the problem. The only way to recover from this is to remove the client computer from the domain, which removes any applied Group Policy settings. Then, before you rejoin the computer to the domain, make sure that the GPO has the required outbound Allow rules.  5. On the Rule Type page, select Predefined, in the drop-down list, select Core Networking, and then click Next.  6. On the Predefined Rules page, make sure that all of the rules are selected, and then click Next.  7. On the Action page, select Allow the connection, and then click Finish.  8. Repeat steps 4 to 7 to add the File and Printer Sharing group of rules.  9. Next, you need to allow lsass.exe to communicate through the firewall for domain authentication purposes. Right-click Outbound Rules, and then click New Rule.  10. On the Rule Type page, click Program, and then click Next.  11. On the Program page, select This program path, and then type %windir%\system32\lsass.exe and then click Next.  12. On the Action page, select Allow the connection, and then click Next.  13. On the Profile page, clear the Private and Public check boxes, and then click Next.  14. On the Name page, type Allow Outbound lsass.exe and then click Finish.  15. If any of your GPOs have WMI filters, you must also create one additional outbound rule to allow the WMIPrvSE.exe program on the client to query the domain controller about the WMI filter and correctly process it. Right-click Outbound Rules, and then click New Rule.  16. On the Rule Type page, click Custom, and then click Next.  17. On the Program page, select This program path, and then type %windir%\system32\wbem\wmiprvse.exe. There are no services to customize in this case so click Next.  18. On the Protocol and Ports page, change Protocol type to TCP, change Remote port to Specific Ports, type 389, and then click Next.  19. On the Scope page, click Next.  20. On the Action page, select Allow the connection, and then click Next.  21. On the Profile page, clear the Private and Public check boxes, and then click Next.  22. On the Name page, type Allow Outbound 389 from WMI Client, and then click Finish.  23. Now that the allow rules are in place, you can enable the default outbound Block rule. In the Group Policy Management Editor click Windows Firewall with Advanced Security - LDAP://{GUID},cn=policies,cn=system,DC=contoso,DC=com, and in the results pane, click Windows Firewall Properties.  24. On the Domain Profile tab, change Outbound connections to Block, and then click OK. |

Now apply the GPO to the client computer to view the effect.

To deploy and test your GPO

|  |
| --- |
| 1. On CLIENT1, at Administrator: Command Prompt, run the command gpupdate /force, and then wait until the command has finished.  2. In an Administrator: Command Prompt, run the command telnet mbrsvr1.  3. The command fails because all outbound network traffic, except for core network traffic and file and printer sharing traffic is blocked. |

In the next section, you create your outbound Allow rule for Telnet.

Next topic:  [Step 2: Allowing Network Traffic for a Program by Using an Outbound Rule](#zfc608cea6af840a3bc626713162abfb3)

Step 2: Allowing Network Traffic for a Program by Using an Outbound Rule

In this step, you create a rule for CLIENT1 to allow outbound traffic on TCP port 23 to reenable the Telnet client program. When creating a rule, we recommend that you be as specific as possible about the program and traffic so that you do not unexpectedly allow or block another program. In this example, you allow the Microsoft Telnet client that is included with Windows, and allow it to use only port 23 outbound.

To create an outbound allow rule

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management Editor, in the Firewall Settings for Windows Clients GPO, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Windows Firewall with Advanced Security, and then expand Windows Firewall with Advanced Security - LDAP://{GUID},cn=policies,cn=system,DC=contoso,DC=com.  2. Right-click Outbound Rules, and then click New Rule.  3. On the Rule Type page, click Custom, and then click Next.  Note  If you select the Port rule type, you can only specify the local port number to allow. We want to allow remote port 23. Therefore, specify the Custom rule type.  4. On the Program page, select This program path, type %windir%\system32\telnet.exe, and then click Next.  5. On the Protocol and Ports page, change the Protocol type to TCP.  6. In the Remote ports list, click Specific Ports, type 23 in the text box, and then click Next.  Note  Be sure to specify the Remote port, not Local. This differs from the inbound rules you set earlier, because this rule applies to the client instead of the server.  7. On the Scope page, click Next.  8. On the Action page, select Allow the connection, and then click Next.  9. On the Profile page, clear the Private and Public check boxes, and then click Next.  10. On the Name page, type Allow Outbound Telnet TCP 23, and then click Finish. |

Now that you have the rule created, deploy it to CLIENT1 and test it.

To deploy and test your outbound allow rule

|  |
| --- |
| 1. On CLIENT1, in an Administrator: Command Prompt, run the command gpupdate /force, and then wait until the command has finished.  2. Run the command telnet mbrsvr1.  3. The connection succeeds because the TCP port 23 traffic can pass outbound through the client’s firewall, and passed inbound through the server’s firewall.  4. Type exit, and then press ENTER to end the Telnet session. |

To simplify the rest of this guide, disable the default outbound block behavior.

To restore the default outbound firewall behavior

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management Editor, (editing Firewall Settings for Windows Clients) right-click Windows Firewall with Advanced Security – LDAP://CN={GUID},cn=policies,cn=system,DC=contoso,DC=com, and then click Properties.  2. On the Domain Profile tab, change Outbound connections to Allow, and then click OK.  3. On CLIENT1, at an Administrator: Command Prompt, run the command gpupdate /force.  4. On CLIENT1, in the Windows Firewall with Advanced Security MMC snap-in, click Windows Firewall with Advanced Security on Local Computer, and then verify that Outbound connections that do not match a rule are allowed is enabled in the Domain profile. |

Next topic: [Deploying a Basic Domain Isolation Policy](#z626058b754b44fc9bbdf7a427bedf467)

Deploying a Basic Domain Isolation Policy

By using Windows Firewall with Advanced Security, you can create connection security rules that specify that traffic must be secured by one or more of the features of IPsec. In domain isolation you use IPsec authentication to require each domain member computer involved in a connection to positively establish the identity of the other computer.

By creating rules that require authentication by a domain member, you effectively isolate those domain-member computers from computers that are not part of the domain.

Computers in a domain isolation environment require authentication for inbound connections. For outbound connections, you typically use the option to request but not require IPsec protection. This enables the computers to protect traffic when communicating with computers that can also use IPsec, but fall back to plaintext when communicating with computers that cannot use IPsec. With Windows XP and earlier versions of Windows, fall back to plain text, when it is enabled, occurs after trying IPsec for three seconds. However, some services have response time-outs that are less than three seconds, which causes them to fail. In these earlier versions of Windows this meant that you had to create (sometimes a very large number of) outbound exemption rules to support those servers or services that cannot authenticate. To address this problem, Microsoft released the Simple Policy Update for Windows Server 2003 and Windows XP. This update reduces the delay for attempts between IPsec-protected clients and non-IPsec-protected clients to one-half second. For more information about the Simple Policy Update for Windows Server 2003 and Windows XP, see [Simplifying IPsec Policy with the Simple Policy Update](http://go.microsoft.com/fwlink/?LinkID=94767) at http://go.microsoft.com/fwlink/?LinkID=94767.

Later versions of Windows improve on this further, and no longer require the update. When you use request mode in Windows Vista and later versions of Windows, Windows sends both connection attempts at the same time. If the remote host responds with IPsec, then the non-IPsec attempt is abandoned. If the IPsec request generates no response then the non-IPsec attempt continues.

This reduced or eliminated delay solves the time-out failure problem for most programs. However, there might still be times when you want to make sure that your computers do not use IPsec to try to talk to certain hosts on the network. In those circumstances, create authentication exemption rules for the clients and they no longer use IPsec to communicate with computers on the exemption list.

For more information about domain isolation, see [Introduction to Server and Domain Isolation](http://go.microsoft.com/fwlink/?LinkID=94631) (http://go.microsoft.com/fwlink/?LinkID=94631) and [Domain Isolation with Microsoft Windows Explained](http://go.microsoft.com/fwlink/?LinkID=94632) (http://go.microsoft.com/fwlink/?LinkID=94632) in the Windows Server Technical Library.

Steps for creating connection security rules to enforce domain isolation

In this section, you create connection security rules that specify that the computers in your domain require authentication for inbound network traffic and request authentication for outbound traffic.

Important

Remember that if you have the default outbound behavior configured to block traffic that does not match an outbound allow rule then you will have to create rules to permit the outbound IPsec network traffic.

[Step 1: Creating a Connection Security Rule that Requests Authentication](#z6d0ac59ef5b34938b93ccbabb45c9e34)

[Step 2: Deploying and Testing Your Connection Security Rules](#ze89cc2d840914537a19786f4923959a1)

[Step 3: Changing the Isolation Rule to Require Authentication](#zed8cc94080c44970997cbbdc16cc3729)

[Step 4: Testing Isolation with a Computer That Does Not Have the Domain Isolation Rule](#z1f83cb3839044a56a66f781083bb3e7f)

[Step 5: Creating Exemption Rules for Computers that are Not Domain Members](#z514c27e7eda046f2be1e43e8168aa70b)

Next topic: [Step 1: Creating a Connection Security Rule that Requests Authentication](#z6d0ac59ef5b34938b93ccbabb45c9e34)

Step 1: Creating a Connection Security Rule that Requests Authentication

In this step, you create connection security rules for the contoso.com domain that cause all member computers to require authentication for inbound network traffic, and request authentication for outbound traffic. You start by using a GPO that only requests inbound authentication, and after you confirm that it is working you revise it to require inbound authentication.

Specifying the IPsec algorithms to use

For simplicity, the rules that you create in the following procedures use the default IPsec main mode and quick mode settings, which specify certain combinations of integrity and encryption algorithms to be included in negotiations. However, Windows provides lots of flexibility in configuring the specific main mode and quick mode algorithms that are used for any given connection. All of the computers that you want to be able to communicate with each other must support at least one set of algorithms in common. If you must use a specific combination of algorithms then you can do one of the following:

 Alter the global IPsec default values. In your GPO, open the Windows Firewall with Advanced Security Properties page, and in the IPsec defaults section, click Customize. You can configure the algorithms used to negotiate protection for both the main mode and quick mode security associations (SAs), and the authentication options available. Changing these settings alters them for all IPsec connections made to and from this computer whose connection security rules do not specify otherwise, and that do not match a main mode rule.

 Create a connection security rule with specific quick mode settings. By using the netsh advfirewall consec add rule command, you can create a connection security rule that includes specific quick mode algorithm combinations. If you specify these in the rule then they are used instead of those in the global IPsec default settings. Use the qmsecmethods parameter. One quick mode option added to Windows 7 and Windows Server 2008 R2 is “Null encapsulation”. This option specifies that no integrity protection is provided to each network packet in the connection. No AH or ESP header is used to encapsulate the data. This option is provided for compatibility with network equipment and software that is incompatible with AH or ESP. You can specify the use of Null encapsulation in either the global IPsec defaults (not recommended), or in a connection security rule that matches only the network traffic that must use Null encapsulation. For more information about how to create connection security rules with custom quick mode settings, see [Netsh AdvFirewall Consec Commands](http://go.microsoft.com/fwlink/?linkid=157374) (http://go.microsoft.com/fwlink/?linkid=157374).

Note

You cannot create a rule with specific quick mode settings by using the Windows Firewall with Advanced Security MMC snap-in.

 Create a main mode rule. Starting with Windows 7 and Windows Server 2008 R2, you can create a rule that specifies main mode encryption, integrity, and authentication settings. Connections that match a main mode rule use the main mode rule settings instead of the settings specified in the connection security rule or the global IPsec defaults. To create a main mode rule, use the netsh advfirewall mainmode add rule command. For more information, see [Netsh AdvFirewall MainMode Commands](http://go.microsoft.com/fwlink/?linkid=147508) (http://go.microsoft.com/fwlink/?linkid=147508).

Firewall and Connection Security integration

One of the big advantages of integrating the firewall functionality with IPsec is the additional options available on a firewall rule. In Windows Vista and later versions of Windows, you can now create firewall rules that filter network traffic based on the following criteria:

 Allow the connection if it is authenticated and integrity-protected. Network traffic that matches this firewall rule must be protected by an IPsec connection security rule that requires both authentication of the connection and the use of an AH or ESP algorithm that helps protect the integrity of each network packet in the connection.

 Require the connection to be encrypted. Network traffic that matches this rule must be encrypted by using an IPsec connection security rule that specifies using ESP encapsulation with encryption. The network traffic must also be authenticated and integrity-protected.

The additional option to Allow the computers to dynamically negotiate encryption enables you to deploy fewer connection security rules to your client computers. For example, to enable encryption for a single port on a server while network traffic to all other ports on the server are unencrypted previously required two rules on both the server and all its clients: one generic rule that applied to all traffic to a server and did not require encryption, and one that specified the server’s IP address and the required port number on the server, and that required encryption. As the number of ports and the number of servers that require this special handling grow, the task of creating and maintaining the required connection security rules becomes more difficult.

By using this option, only the generic rule that requires authentication and integrity is required on the clients. On the server only, you create a firewall rule for the specific port number that requires encryption, and that enables dynamic encryption. The main mode SA can therefore be negotiated by using the single rule on the client. When the client sends traffic to the specified port number protected by the firewall rule, the server starts a quick mode negotiation with the client to create an “upgraded” SA that requires encryption. Any encryption algorithm combinations enabled in the global IPsec defaults for quick mode negotiations can be used. In addition to being able to specify a port, you can alternatively create a firewall rule that requires encryption only for a specified service, program executable, or protocol. All network traffic to other services, other programs, or that use other protocols on the computer would not trigger a quick mode SA negotiation to require encryption.

Although this option was introduced with Windows 7 and Windows Server 2008 R2, it is compatible with computers that are running Windows Vista and Windows Server 2008 and can be applied to them by using Group Policy.

 Allow the connection to use null encapsulation.. This option specifies that after main mode negotiation and authentication is completed, the quick mode SA requires no AH or ESP encapsulation. The data stream for the connection therefore does not receive per-packet integrity protection. This option is provided for compatibility with network equipment or software that is incompatible with AH or ESP.

To create a new GPO for domain isolation

|  |
| --- |
| 1. On MBRSV1, in Group Policy Management, right-click Group Policy Objects, and then click New.  2. In Name, type Domain Isolation, and then click OK.  3. In the navigation pane, right-click your new GPO, and then click Edit.  4. In Group Policy Management Editor, in the navigation pane, right-click the top node for your Domain Isolation GPO, and then click Properties.  5. Select the Disable User Configuration settings check box, because this is a computer-only GPO.  6. In the Confirm Disable dialog box, click Yes, and then click OK.  7. In the navigation pane, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Windows Firewall with Advanced Security, and then expand Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com.  8. Right-click Connection Security Rules, and then click New rule.  9. On the Rule Type page, click Isolation, and then click Next.  10. On the Requirements page, confirm that Request authentication for inbound and outbound connections selected, and then click Next.  Caution  In a production environment, we recommend that you set request mode first and allow the GPO to fully propagate to the network. Confirm that all your computers are communicating successfully by using IPsec before changing the rules to require mode. Setting the rule to require mode first can result in computers that cannot communicate until all the computers receive and apply the GPO. In a later step, you modify the rule to change it to require inbound authentication.  11. On the Authentication Method page, click Computer and user (Kerberos V5), and then click Next.  Note  Although you typically do not filter by user credentials in domain isolation, user authentication in addition to computer authentication enhances security, and makes implementing server isolation based on a user’s identity later much easier, because a compatible authentication method is already in place.  12. On the Profile page, clear the Private and Public check boxes, and then click Next.  13. On the Name page, type Request Inbound Request Outbound, and then click Finish. |

Next topic: [Step 2: Deploying and Testing Your Connection Security Rules](#ze89cc2d840914537a19786f4923959a1)

Step 2: Deploying and Testing Your Connection Security Rules

In this step, you deploy and test your domain isolation rule. You link the GPO that contains the rule to the OUs that contain the computer accounts, and then you test connectivity and view the IPsec security associations (SAs) that are created to support the connection.

Start by linking your GPO to the OUs that contains the computers to receive the rule.

To link your GPO to the appropriate OUs

|  |
| --- |
| 1. On MBRSVR1, open the Group Policy Management snap-in.  2. Right-click MyClientComputers, and then click Link an Existing GPO.  3. In the Group Policy objects list, select Domain Isolation, and then click OK.  4. Right-click MyMemberServers, and then click Link an Existing GPO.  5. In the Group Policy objects list, select Domain Isolation, and then click OK.  If you browse your OUs, you see a list that resembles the following diagram: |

Important

Do not apply the domain isolation GPOs to domain controllers.

Note

In the previous procedure, you did not use WMI or security group filters because of the simplicity of the lab setup used in this guide, and because it is not important to what is being demonstrated here. However, in a production environment, make sure that your GPOs are carefully deployed using appropriate WMI and security group filters to only the desired target computers.

Now, make sure that both computers receive and apply the new GPO.

To test the new GPO on your computers

|  |
| --- |
| 1. On both MBRSVR1 and CLIENT1, at an Administrator: Command Prompt, run gpupdate /force. Wait until the commands finish.  2. On CLIENT1, at the command prompt, run telnet mbrsvr1.  The connection succeeds. Do not end the Telnet session yet.  3. Open the Windows Firewall with Advanced Security snap-in.  4. Expand Monitoring, expand Security Associations, and then click Main Mode.  5. In the Main Mode pane, double-click the security association (SA) that is displayed.  6. Examine the settings, as shown in the following figure, that the local computer (CLIENT1) negotiated with the remote computer (MBRSVR1). The specific algorithms displayed might vary depending on whether you use Windows 7 or Windows Vista on CLIENT1, and Windows Server 2008 R2 or Windows Server 2008 for MBRSVR1.    7. Click OK.  8. In the navigation pane, click Quick Mode, and then double-click the SA that is displayed.  9. Examine the settings, which show that any traffic between the two computers using any protocol is protected using the Encapsulating Security Payload (ESP) integrity algorithm Secure Hash Algorithm (SHA-1). ESP integrity uses a cryptographically protected checksum to ensure that the packets that are received have not been modified after they are sent. Any packets that fail the integrity tests are silently dropped.  Note  SAs have a limited lifetime. Therefore, if you let the connection sit idle long enough, the SA can expire and be removed from the list. By sending more network traffic, the SA is automatically renegotiated and reappears in the list.  10. Type exit at the Telnet prompt to end the Telnet session. |

Next topic: [Step 3: Changing the Isolation Rule to Require Authentication](#zed8cc94080c44970997cbbdc16cc3729)

Step 3: Changing the Isolation Rule to Require Authentication

In this step, modify the rule that you created so that authentication is required instead of requested. After you complete this step, clients that cannot authenticate or that do not have a connection security rule to authenticate the traffic, cannot communicate with computers that are domain members.

Caution

In a production environment, only perform this procedure after confirming that all the clients and servers are communicating by using the IPsec settings in the “request” version of the rule. If you change the rule to “require” before confirming that your computers can communicate successfully using its settings then you might unintentionally put your computers in a state where they cannot communicate.

To change the policy from requesting to requiring authentication

|  |
| --- |
| 1. On MBRSVR1, switch to the Group Policy Management Editor.  2. In the results pane, right-click Request Inbound Request Outbound, and then click Properties.  3. In the Name text box, change the name to Require Inbound Request Outbound to accurately reflect its new behavior.  4. Click the Authentication tab.  5. Under Requirements, change Authentication mode to Require inbound and request outbound, and then click OK.  Note  Although using Require inbound and outbound would work for this guide, in a production environment it is usually not practical to require outbound authentication. Domain-member computers often must initiate communications with computers that are not in the domain, such as remote Web sites. |

Confirm that the computers can still communicate even though authentication is required.

To test the modified GPO requiring authentication

|  |
| --- |
| 1. On both MBRSVR1 and CLIENT1, at an Administrator: Command Prompt, run gpupdate /force.  2. On CLIENT1, at the command prompt, run telnet mbrsvr1.  The connection succeeds.  3. Type exit to end the Telnet session. |

Next topic: [Step 4: Testing Isolation with a Computer That Does Not Have the Domain Isolation Rule](#z1f83cb3839044a56a66f781083bb3e7f)

Step 4: Testing Isolation with a Computer That Does Not Have the Domain Isolation Rule

To simulate a computer that is not part of the domain, remove the GPO from CLIENT1, and try to connect again.

To remove the GPO from CLIENT1

|  |
| --- |
| 1. On MBRSVR1, switch to Group Policy Management.  2. Under MyClientComputers, right-click Domain Isolation, and then click Link Enabled to disable the link. |

In the next procedure, you refresh the GPO on CLIENT1 and try to communicate with MBRSVR1.

To test the modified GPO on CLIENT1

|  |
| --- |
| 1. On CLIENT1, at an Administrator: Command Prompt, run gpupdate /force. Wait until the command finishes.  2. At the command prompt, run telnet mbrsvr1. The connection fails because it never receives a reply to its request. Because MBRSVR1 requires authentication, and CLIENT1 cannot supply it, all incoming packets are dropped. |

In the next procedure, you restore the GPO to the client so that the correct rule is in place for later steps.

To reapply the GPO to CLIENT1

|  |
| --- |
| 1. On MBRSVR1, under MyClientComputers, right-click Domain Isolation, and then click Link Enabled.  2. If you want, you can repeat the previous procedure "To test the modified GPO on CLIENT1" to confirm that you can connect again. This time the connection succeeds. |

Next topic: [Step 5: Creating Exemption Rules for Computers that are Not Domain Members](#z514c27e7eda046f2be1e43e8168aa70b)

Step 5: Creating Exemption Rules for Computers that are Not Domain Members

In this step, you add a rule to your domain isolation GPO to exempt all DNS servers on the network from the domain isolation authentication requirements.

Note

DNS is used here to serve as a simple example. If the computers on the network are all running Windows Vista or later versions of Windows, or if they can run the [Simple Policy Update for Windows Server 2003 and Windows XP](http://go.microsoft.com/fwlink/?LinkID=94767) (http://go.microsoft.com/fwlink/?LinkID=94767), then you typically do not need to add DNS exemption rules as illustrated here in a production environment. Fewer exemption rules means less complexity for your connection security and firewall rule GPOs. Create exemption rules only for those services that need them.

To modify your domain isolation GPO to exempt DNS servers

|  |
| --- |
| 1. On MBRSVR1, switch to the Group Policy Management Editor that has the Domain Isolation GPO open.  2. In the navigation pane, navigate to and expand Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com, right-click Connection Security Rules, and then click New rule.  3. On the Rule Type page, click Authentication exemption, and then click Next.  4. On the Exempt Computers page, click Add.  5. In the IP Address dialog box, click Predefined set of computers.  6. Click the list to expand it, select DNS servers, and then click OK.  Note  As implemented on the client computer that receives this GPO, DNS Servers is interpreted to mean the DNS servers that are currently configured on the client computer.  7. Back on the Exempt Computers page, click Next.  8. On the Profile page, clear the Private and Public check boxes, and then click Next.  9. On the Name page, type Exempt DNS servers from domain isolation, and then click Finish.  The new rule appears in your GPO.  Note  You can use a network traffic analyzer such as Microsoft Network Monitor to see the network packets before and after you apply this rule to confirm that IPsec attempts are not made to the DNS server after the exemption rule is applied. To download Network Monitor, see [Microsoft Network Monitor](http://go.microsoft.com/fwlink/?LinkID=94770) at http://go.microsoft.com/fwlink/?LinkID=94770. Look for the download links in the left-hand column. |

Next topic: [Isolating a Server by Requiring Encryption and Group Membership](#zfb995b0bce8b4507a6531acdf5ef8ff5)

Isolating a Server by Requiring Encryption and Group Membership

Domain isolation restricts domain-member computers to requiring authentication when communicating with other domain-member computers, and rejecting inbound connections that are not authenticated. This helps improve the security of most of the computers in your organization. Some servers, however, contain sensitive data, such as personal data, medical records, or credit card data that must be guarded even more carefully. In many cases government regulations specify that this data must be protected to make sure that only those users who have business need can physically get access to the data. You can use IPsec to provide this additional layer or protection in the form of server isolation. By using server isolation, you can further restrict access to sensitive data not just to unspecified domain member computers and users, but only those users and computers that have a legitimate business need. Often such data must also be encrypted during transmission to prevent eavesdropping.

By using Windows Firewall with Advanced Security, you can specify that specific network connections can be accessed only by specific users, based on their group membership. You can also specify that access is permitted only by specific computers based on computer account membership in a group. Both types of restriction are based on the authentication methods demonstrated in the previous section. Finally, you can also specify that these network connections must be encrypted by using one of several encryption algorithms.

For more information about server isolation, see:

 [Introduction to Server and Domain Isolation](http://go.microsoft.com/fwlink/?LinkID=94631) at http://go.microsoft.com/fwlink/?LinkID=94631

 [Server Isolation with Microsoft Windows Explained](http://go.microsoft.com/fwlink/?LinkID=94793) at http://go.microsoft.com/fwlink/?LinkID=94793

Steps for creating connection security rules to enforce server isolation

In this section, you create inbound firewall rules that specify that only users who are members of a specific group can access MBRSVR1. You also configure the rules to require encryption for all connections to the specified server.

[Step 1: Creating the Security Group](#zceade705067c4ab3ad3da138ee9489a9)

[Step 2: Modifying a Firewall Rule to Require Group Membership and Encryption](#z8cb3988365254cfb8e0c227ee5e3e2de)

[Step 3: Creating a Firewall Rule for the Client to Support Encryption](#z41a7a2c6dd53435a8daca9aa12cbc183)

[Step 4: Testing the Rule When Admin1 Is Not a Member of the Group](#za97ebb6b9885469d831b85f341336412)

[Step 5: Adding Admin1 to the Group and Testing Again](#zfa4679b80ce942b3a63796637e0285e4)

Note

In some environments, you might want to implement server isolation without domain isolation. This guide demonstrates server isolation as an additional layer added to domain isolation. To deploy server isolation by itself, you still must create and deploy authentication requesting connection security rules. But instead of deploying them to all computers in the organization, you only need to deploy them to the servers that are to be isolated, and to the client computers that are used to access the servers. You can do this by deploying the authentication connection security rules with the same security group filter as is demonstrated in this section.

Next topic: [Step 1: Creating the Security Group](#zceade705067c4ab3ad3da138ee9489a9)

Step 1: Creating the Security Group

In this step, you create a security group in Active Directory. This group will be referenced by your firewall rule in a later step to control which users can access the server.

Note

Although this guide only demonstrates server isolation by using user accounts, a very similar process can be followed to restrict access from only authorized computers. To restrict access by either, you must use an authentication method that includes the appropriate credentials. In the previous section on domain isolation, you created a rule that requests both user and computer authentication using Kerberos V5, which is perfect for our purposes in this section on server isolation.

To create a security group

|  |
| --- |
| 1. On DC1, click Start, click Administrative Tools, and then click Server Manager.  2. In the navigation pane, expand Roles, expand Active Directory Domain Services, expand Active Directory Users and Computers, expand contoso.com, right-click Users, click New, and then click Group.  3. In the New Object - Group dialog box, in the Group name text box, type Authorized to Access MBRSVR1, and then click OK.  4. Leave Server Manager running with the Computers container shown in the results pane. |

Do not add any users to the group yet.

Next topic: [Step 2: Modifying a Firewall Rule to Require Group Membership and Encryption](#z8cb3988365254cfb8e0c227ee5e3e2de)

Step 2: Modifying a Firewall Rule to Require Group Membership and Encryption

Server isolation takes the connection security rule that enforces authentication, and layers a firewall rule that additionally restricts the traffic to only authorized users or computers. In this step, you modify your Telnet firewall rule to allow Telnet traffic only from users who are members of the security group you created in the last step. Because the authentication that is currently configured, you could decide to restrict access based either on the computer, the user, or both. In this example, you configure the firewall rule to restrict access to user accounts that are approved.

To modify the Telnet firewall rule on MBRSVR1

|  |
| --- |
| 1. On MBRSVR1, switch to Group Policy Management.  2. In the navigation pane, under Group Policy Objects, right-click Firewall Settings for Windows Servers, and then click Edit.  3. In the Group Policy Management Editor, under Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Windows Firewall with Advanced Security, expand Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com, and then click Inbound Rules.  4. In the results pane, right-click Allow Inbound Telnet, and then click Properties.  5. Change the name by typing Allow Encrypted Inbound Telnet to Group Members Only.  6. Perform one of the following:   If you are running Windows Server 2008 R2: Select Allow the connection if it is secure, click Customize, select Require the connections to be encrypted, and then click OK.   If you are running Windows Server 2008: Select Allow only secure connections, and then click Require encryption.  7. Perform one of the following:   If you are running Windows Server 2008 R2: Click the Users tab.   If you are running Windows Server 2008: Click the Users and Computers tab.  8. Under Authorized users, select Only allow connections from these users, and then click Add.  9. In the Select User or Groups dialog box, type Authorized to Access MBRSVR1, click Check Names to make sure that it resolves, and then click OK.  Important  Even though this guide only demonstrates how to use a user group, remember that you can also specify computer group membership as a requirement, as long as the authentication method that is used includes computer authentication in addition to user authentication. This enables you to specify that only users who are members of group X can access the protected server, and only when they are using a computer that is a member of group Y. An authorized user who uses a non-authorized computer cannot access the protected server, nor can an authorized computer be used by a non-authorized user to access the protected server.  10. Click OK to close the Allow Inbound Telnet Properties page.  11. Close the Group Policy Management Editor. |

Next topic: [Step 3: Creating a Firewall Rule for the Client to Support Encryption](#z41a7a2c6dd53435a8daca9aa12cbc183)

Step 3: Creating a Firewall Rule for the Client to Support Encryption

In this step, you create a new firewall rule that applies to the client computer so that it can successfully encrypt the connection as required by the server.

To create a Telnet firewall rule that requires authentication for the client

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management, under Group Policy Objects, right-click Firewall Settings for Windows Clients, and then click Edit.  2. In the Group Policy Management Editor, expand Policies, expand Windows Settings, expand Security Settings, expand Windows Firewall with Advanced Security, expand Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com, right-click Outbound Rules, and then click New Rule.  3. On the Rule Type page, click Custom, and then click Next.  4. On the Program page, click All Programs, and then click Next.  Note  By restricting the rule to the Telnet port number (in the next step), instead of the program name, any correctly configured Telnet client can be used. If you specify a program by path and file name then only that specific program works, and other Telnet client programs fail. This configuration is recommended only for outbound rules. For inbound rules, we recommend that you use both a port restriction and a program restriction. That way the port is only open when the program is running. If you do not specify a program then the port remains open all the time.  5. On the Protocol and Ports page, change the Protocol type to TCP.  6. Change the Remote port list to Specific Ports, type 23 in the text box, and then click Next.  7. On the Scope page, under Which remote IP addresses does this rule match, select the These IP addresses check box. Make sure to select the option under remote.  8. To the right of the Remote address section, click Add.  9. In the IP Address dialog box, type 192.168.0.100 (the IP address of MBRSVR1) in the top text box, click OK, and then click Next.  Important  Adding the IP address of the server makes this rule more specific than the outbound Telnet rule that you created earlier. When two rules potentially match a connection, the most specific one is select. This means that when you try to Telnet to 192.168.0.100, the authentication and encryption requirements are enforced. If you Telnet to any other server, the other rule is matched and authentication and encryption are not required.  10. Perform one of the following:   If you are running Windows Server 2008 R2: On the Action page, select Allow the connection if it is secure, click Customize, select Require the connections to be encrypted, click OK, and then click Next.   If you are running Windows Server 2008: On the Action page, select Allow the connection if it is secure, click Require the connections to be encrypted, and then click Next.  11. On the Computers page, click Next.  12. On the Profile page, clear the Private and Public check boxes, and then click Next.  13. Name the rule Allow only encrypted Telnet to MBRSVR1, and then click Finish.  14. At an Administrator: Command Prompt, run gpupdate /force. Wait until the command finishes. |

Next topic: [Step 4: Testing the Rule When Admin1 Is Not a Member of the Group](#za97ebb6b9885469d831b85f341336412)

Step 4: Testing the Rule When Admin1 Is Not a Member of the Group

CLIENT1 has a firewall rule and a connection security rule that meet all the requirements to communicate with MBRSVR1, but Admin1 has not yet been added to the user group that is referenced in the inbound Telnet firewall rule for MBRSVR1. In this step, you try to connect to the Remote Event Viewer service to demonstrate that your new rules do not affect services other than Telnet. You also attempt to connect to the Telnet service on MBRSVR1 to see that the new rules prevent you from accessing the Telnet service because you are not a member of the required group.

To try to connect to the Remote Event Viewer service on MBRSVR1

|  |
| --- |
| 1. On CLIENT1, at an Administrator: Command Prompt, run gpupdate /force. Wait until the command finishes.  2. Click Start, type event viewer in the Start Search box, and then press ENTER.  3. In the navigation pane of Event Viewer, right-click the top node Event Viewer (Local), and then click Connect to another computer.  4. In the Select Computer dialog box, type MBRSVR1, and then click OK.  The attempt is successful, because the rules you created do not require group membership or encryption for the Event Viewer. |

Now, to see the effect of your new rules, try to connect to MBRSVR1 using Telnet.

To try to connect to MBRSVR1 by using Telnet

|  |
| --- |
|  On CLIENT1, at an Administrator: Command Prompt, run telnet mbrsvr1.  The command fails because Admin1 is not yet a member of the Authorized to Access MBRSVR1 group, and only members of that group are permitted to send port 23 traffic through Windows Firewall with Advanced Security to that server. |

Next topic: [Step 5: Adding Admin1 to the Group and Testing Again](#zfa4679b80ce942b3a63796637e0285e4)

Step 5: Adding Admin1 to the Group and Testing Again

In this step, you add your user account Admin1 to the security group Authorized to Access MBRSVR1, and then verify that it enables the client to access the Telnet service again.

To add Admin1 to the group

|  |
| --- |
| 1. On DC1, in the Users container, double-click the group Authorized to Access MBRSVR1, and then click the Members tab.  2. Click Add.  3. In the Select Users, Contacts, Computers, or Groups dialog box, in the text box, type Admin1 and then click OK.  4. Click OK to close the group Properties page. |

To test Telnet access from CLIENT1 to MBRSVR1

|  |
| --- |
| 1. Because Admin1’s group membership must be refreshed, you must log off and log on again. On CLIENT1, log off, and then log on as contoso\admin1.  2. Open an Administrator: Command Prompt, and then run gpupdate /force. When you logged off and back on, user policy is refreshed; this step refreshes computer policy.  3. At the command prompt, run telnet mbrsvr1  The command works because all requirements of the rules are now satisfied. Only computers that are a member of the domain and users that authenticate as a member of the specified group can access the Telnet service on MBRSVR1.  4. Open the Windows Firewall with Advanced Security snap-in.  5. Expand Monitoring, expand Security Associations, and then click Quick Mode.  6. Double-click the SA to display its properties. There is now a protocol listed next to ESP encryption (Windows 7) or ESP confidentiality (Windows Vista). That is the encryption algorithm being used by this connection.  The encryption settings that are used are determined by the IPsec defaults. You can find these by opening the Windows Firewall with Advanced Security Properties dialog box, and then select the IPsec Settings tab. Under IPsec defaults click Customize, under Data protection (Quick Mode), select Advanced, and then click Customize. The algorithm combination (called a quick mode proposal) in the Data integrity and encryption column that is highest on the list and that matches a proposal on the remote server is the one used.  7. Click OK to close the SA, and then close Windows Firewall with Advanced Security.  8. In the Telnet window, type exit, and then press ENTER to end the Telnet session. |

Next topic: [Creating Firewall Rules that Allow IPsec-protected Network Traffic (Authenticated Bypass)](#zd9891d8917d74cf3a08de4a46904a7a2)

Creating Firewall Rules that Allow IPsec-protected Network Traffic (Authenticated Bypass)

In a typical network, you want all network traffic blocked except for traffic that is truly required.

To help strengthen security, by default, rules that block traffic have a higher precedence than rules that allow traffic. So if traffic coming into (or going out of) the firewall matches both an allow rule and a block rule, the block rule takes precedence, and the traffic will be dropped.

There are times however, when you might want to allow network traffic into a computer that would ordinarily be blocked. For example, the network troubleshooting team might need to use network protocol analyzers or other network troubleshooting equipment in ways that the firewall rules would ordinarily prevent. In such circumstances, you can create a special type of allow rule that overrides a block rule when the network traffic meets certain administrator specified requirements.

These rules are referred to as “authenticated bypass” rules. If you enable the Override block rules setting on the firewall rule then correctly authenticated traffic that matches this rule is permitted, even if another rule would block it. The result is a set of rules that say "this traffic is blocked unless it is coming from an authorized computer."

Steps for creating rules that allow specific computers or users to bypass the firewall

In this section of the guide, you create a firewall rule that blocks all Telnet network traffic, and then test it with your existing Telnet allow rule you created in a previous section to see that the block rule takes precedence. Then you modify your existing Telnet allow rule to include the Override Block Rules setting, and confirm that you can connect from your approved computer.

[Step 1: Adding and Testing a Firewall Rule that Blocks Standard Telnet Traffic](#z54df1225b1334ef5bae98c3027bf6f77)

[Step 2: Modifying a Telnet Firewall Allow Rule to Override Block Rules](#zdbaf9cad693a4b3495beb78009aed835)

Next topic: [Step 1: Adding and Testing a Firewall Rule that Blocks Standard Telnet Traffic](#z54df1225b1334ef5bae98c3027bf6f77)

Step 1: Adding and Testing a Firewall Rule that Blocks Standard Telnet Traffic

Create a rule that blocks all Telnet traffic, and then test it against the existing Telnet allow rule to see that the cumulative effect is to block Telnet traffic.

To create a Telnet block rule

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management, click Group Policy Objects, right-click Firewall Settings for Windows Servers, and then click Edit.  2. In the Group Policy Management Editor, in the navigation pane, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Windows Firewall with Advanced Security, and then expand Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com.  3. Right-click Inbound Rules, and then click New Rule.  4. On the Rule Type page, click Custom, and then click Next.  5. On the Program page, click This program path, and then in the text box, type %systemroot%\system32\tlntsvr.exe.  6. Click Customize, click Apply to this service, click the row for Telnet with a short name of TlntSvr, click OK, and then click Next.  7. On the Protocol and Ports page, change the Protocol type to TCP, change Local port to Specific Ports, type 23 in the text box, and then click Next.  8. On the Scope page, click Next.  9. On the Action page, click Block the connection, and then click Next.  10. On the Profile page, clear the Private and Public check boxes, and then click Next.  11. On the Name page, type Block All Telnet, and then click Finish. |

Now you have two conflicting rules. One specifies that Telnet traffic is permitted as long as it is encrypted and sent by a user that is a member of the group Authorized to Access to MBRSVR1. The other rule says to block all Telnet traffic. In the next procedure you see what Telnet connectivity is available when these two rules are both in place.

To test Telnet connectivity when two conflicting rules are in place

|  |
| --- |
| 1. On MBRSVR1, switch to the Administrator: Command Prompt, run gpupdate /force. Wait until the command is finished.  2. On CLIENT1, at a command prompt, type the command telnet mbrsvr1.  The command fails because the inbound block rule has a higher precedence than the inbound allow rule. |

Next topic: [Step 2: Modifying a Telnet Firewall Allow Rule to Override Block Rules](#zdbaf9cad693a4b3495beb78009aed835)

Step 2: Modifying a Telnet Firewall Allow Rule to Override Block Rules

In this step, you modify your existing Telnet allow rule to include the Override Block Rule setting, and then test the behavior of Telnet with the modified rule. This works because you already have a connection security rule that authenticates and encrypts all Telnet traffic.

To add the Override Block Rule setting to your rule

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management Editor, click Inbound Rules.  2. Right-click Allow Encrypted Inbound Telnet to Group Members Only, and then click Properties.  3. Authenticated bypass rules must specify at least one authorized computer or computer group. On the Computer tab, select Only allow connections from these computers, and then click Add.  4. For our simple example, type domain computers, and then click OK. This restricts access to computers that are domain members. Remember that we are already restricting access to users who are members of a group.  5. Perform one of the following:   If you are running Windows Server 2008 R2, on the General tab, in the Action section, click Customize. On the Customize Allow if Secure Settings dialog box, select Override block rules, and then click OK two times.   If you are running Windows Vista: On the General tab, in the Action section, select the Override block rules check box, and then click OK two times. |

Now test the two conflicting rules.

To test the Telnet connectivity with your current rule configuration

|  |
| --- |
| 1. On MBRSVR1, at an Administrator: Command Prompt, run gpupdate /force. Wait until the command is finished.  2. On CLIENT1, at a command prompt, run telnet mbrsvr1.  The command succeeds because the existing Telnet allow rule now overrides the block rule. The only traffic that can bypass the Telnet block rule is traffic that matches the authenticated bypass Telnet allow rule. That rule specifies that the traffic must be authenticated, and in this case, encrypted. Traffic from any computer or user not on the authorized list, or traffic that is not authenticated or encrypted is dropped.  3. Type exit and the press ENTER to end the Telnet session. |

Next topic: [Creating Tunnel Mode IPsec Rules](#ze8e462c96d324ce89d07080a9f7f2b19)

Creating Tunnel Mode IPsec Rules

IPsec tunnel mode rules can be used to create secured network connections across the Internet to private networks, or to connect two private networks that are separated by the Internet.

In earlier versions of Windows, creating IPsec rules for client-to-gateway type rules were easy to deploy on the gateway server, but difficult to deploy to the clients. This was because in these IPsec rules you needed to specify both ends of the tunnel by an explicit IP address, and both sets of computers at either end of the tunnel that are accessible through the tunnel. This meant that you had to have a customized rule for each client that you wanted enabled to connect to the gateway. Starting with Windows Server 2008 R2 and Windows 7, however, you can use the “Any” keyword for both the local endpoint and the local tunnel endpoint. When this rule is deployed on the client, “Any” is interpreted to mean the local computer’s own IP address. This enables you to deploy a single rule to all of the clients that have only the remote tunnel endpoint computer’s IP address, and the IP addresses of the computers accessible beyond the gateway.

Important

This scenario uses features that are new to Windows 7 and Windows Server 2008 R2. If you are running Windows Vista on CLIENT1, or Windows Server 2008 on MBRSVR1 then you cannot complete this scenario.

Steps for creating rules that create a client-to-gateway IPsec tunnel

In this section of the guide, you reconfigure the lab computers to enable a multiple network remote access scenario. CLIENT1 becomes a remote client on test “public” network, and MBRSVR1 becomes an IPsec gateway server with the addition of a second network adapter so that it can attach to both the new public network and the original private network used in the previous scenarios. DC1 continues to operate on the private network, and serves as the destination server.

[Step 1: Reconfigure your Lab Computers to Support the IPsec Client-to-Gateway Scenario](#ze74393792a024114a7cadb64c5fcbf71)

[Step 2: Create the Connection Security Rules for the Remote Client and IPsec Gateway](#z210cbc16d6df45c386c347baf3ad5287)

[Step 3: Test Your Tunnel Mode Rules](#z68212fa516504a9ab28198a0f2df7ac5)

Next topic: [Step 1: Reconfigure your Lab Computers to Support the IPsec Client-to-Gateway Scenario](#ze74393792a024114a7cadb64c5fcbf71)

Step 1: Reconfigure your Lab Computers to Support the IPsec Client-to-Gateway Scenario

Important

The procedures in this topic use features that are new to Windows 7 and Windows Server 2008 R2. If you are running Windows Vista on CLIENT1, or Windows Server 2008 on MBRSVR1 then you cannot complete this scenario.

For the previous scenarios, all three of your computers were on a single subnet, with IP addresses of 192.168.0.xyz. In the following procedure, you move CLIENT1 to a different network that represents the public Internet. You also configure a second network adapter on MBRSVR1 to connect to the same public network. This enables MBRSVR1 to act as an IPsec gateway, providing access from CLIENT1 to the private network on which DC1 resides. You also remove the GPOs that were developed for the previous scenarios so that you can work locally on CLIENT1 and MBRSVR1.

To remove the GPOs for the previous scenarios

|  |
| --- |
| 1. On MBRSVR1, in Group Policy Management, under Group Policy Objects, right-click Firewall Settings for Windows Clients, and then click Delete.  2. On the confirmation dialog box, click OK.  3. Repeat steps 1 and 2 for the Firewall Settings for Windows Servers and the Domain Isolation GPOs. Do not delete the Default Domain Policy or Default Domain Controllers Policy.  4. On both MBRSVR1 and CLIENT1, run the command gpupdate /force. This removes the GPOs from those computers and removes all of the restrictions caused by them. |

To reconfigure CLIENT1

|  |
| --- |
| 1. Disconnect the network cable connecting CLIENT1 to the private network that connects MBRSVR1 and DC1, and then connect it to a switch for a separate network. If you are using virtual machines (VMs) for this guide then create a separate virtual network and connect the network adapter on CLIENT1 to it.  2. On CLIENT1, click Start, click Control Panel, and then under Network and Internet click View Network status and tasks.  Network and Sharing Center appears.  3. In the navigation pane, click Change adapter settings.  4. In the Network Connections window, right-click the network adapter, and then click Properties.  5. On the Properties dialog box of the network adapter, select Internet Protocol Version 4 (TCP/IPv4), and then click Properties.  6. Change the IP address for the adapter to 131.107.0.101, change the Subnet mask to 255.255.255.0, and then change the Default Gateway to 131.107.0.100. Leave the DNS Server fields unchanged, and then click OK two times to save your settings. |

Now configure MBRSVR1.

To reconfigure MBRSVR1

|  |
| --- |
| 1. If you have not yet done so, shut down Windows, and then install a second network adapter in MBRSVR1. If you are using VMs for this guide then shut down Windows and use your VM administration console to configure a second network adapter for MBRSVR1.  2. Connect the network cable from the new network adapter to the same network as CLIENT1. If you are using VMs for this guide then connect the adapter to the same virtual network as CLIENT1.  3. Restart MBRSVR1, and then log on as contoso\admin1.  4. On MBRSVR1, click Start, click Control Panel, and then under Network and Internet click View Network status and tasks.  Network and Sharing Center appears.  5. In the navigation pane, click Change adapter settings.  6. In the Network Connections window, right-click the new network adapter, and then click Properties.  7. On the Properties dialog box of the network adapter, select Internet Protocol Version 4 (TCP/IPv4), and then click Properties.  8. Select Use the following IP address.  9. Change the IP address for the adapter to 131.107.0.100, and a Subnet mask of 255.255.255.0.  10. Click OK to save your settings. |

The only change you must make on DC1 is to set the default gateway to point to MBRSVR1.

To reconfigure DC1

|  |
| --- |
| 1. On DC1, click Start, click Control Panel, and then under Network and Internet, click View Network status and tasks.  Network and Sharing Center appears.  2. In the navigation pane, click Change adapter settings.  3. In the Network Connections window, right-click the network adapter, and then click Properties.  4. On the Properties dialog box of the network adapter, select Internet Protocol Version 4 (TCP/IPv4), and then click Properties.  5. Change the Default Gateway to 192.168.0.100. Leave the all of the other fields unchanged, and then click OK and Close to save your settings. |

The next step enables IP packet forwarding on MBRSVR1 so that packets arriving at the end of the tunnel are forwarded on to the private network and vice versa.

To enable packet forwarding on MBRSVR1

|  |
| --- |
| 1. On MBRSVR1, at Administrator: command prompt, run the following two commands:  netsh interface ipv4 set interface “local area connection” forwarding = enabled  netsh interface ipv4 set interface “local area connection 2” forwarding = enabled |

By default, the ICMP protocol that is used by ping is blocked by the firewall so the next step is to enable ICMP on CLIENT1 and MBRSVR1 so that we can verify connectivity. ICMP is already enabled on DC1 because of the Active Directory rules that are automatically enabled when the role service is installed.

To enable ICMP traffic on MBRSVR1 and CLIENT1

|  |
| --- |
| 1. On MBRSVR1, start Windows Firewall with Advanced Security.  2. Click Inbound Rules, right-click the rule File and Printer Sharing (Echo Request – ICMPv4-In), and then click Enable Rule.  3. Repeat steps 1 and 2 on CLIENT1 to enable the same rule on that computer. On CLIENT1, there are two versions of the rule – one for the Domain profile, and one for the Public and Private profiles. Enable both rules.  4. Now you can confirm connectivity on your new network. On CLIENT1, at a command prompt, run the command ping 192.168.0.1. Confirm that you receive replies from MBRSVR1.  Note  You have to use the IP address, because CLIENT1 currently cannot communicate with the DNS server on the private network.  5. On DC1, at a command prompt, run the command ping 131.107.0.101, and confirm that you receive a reply from CLIENT1.  Tip  You may need to restart CLIENT1 for this to work. |

Next topic: [Step 2: Create the Connection Security Rules for the Remote Client and IPsec Gateway](#z210cbc16d6df45c386c347baf3ad5287)

Step 2: Create the Connection Security Rules for the Remote Client and IPsec Gateway

You now have a client on a “public” network, and a server that is dual-homed on the “public” network with the client computer, and the “private” network with the domain controller. Because the client does not have access to the domain controller to receive Group Policy updates, you must create the tunnel mode IPsec rules manually.

Important

This section of the guide uses features that are present only on computers that are running Windows 7 and Windows Server 2008 R2, and will not work as written on computers that are running earlier versions of Windows.

To create the tunnel mode rule on CLIENT1

|  |
| --- |
| 1. On CLIENT1, start the Windows Firewall with Advanced Security MMC snap-in.  2. Right-click Connection Security Rules, and then click New Rule.  3. On the Rule Type page, select Tunnel, and then click Next.  4. On the Tunnel Type page, select Client-to-gateway, and then click Next.  5. On the Requirements page, select Require authentication for inbound and outbound connections, and then click Next.  6. On the Tunnel Endpoints (Client-to-Gateway) page, in Remote tunnel endpoint, type the IPv4 address of MBRSVR1: 131.107.0.100.  Note that you do not have to specify the local tunnel endpoint; it is already configured as My IP address. This is a new feature of Windows 7 and Windows Server 2008 R2 that simplifies GPO deployment, because this rule matches all clients of the gateway server. You no longer have to deploy multiple rules with specific local tunnel endpoint settings for each client computer.  7. Under What are the remote endpoints?, click Add.  8. Type the subnet identifier for the private network behind the gateway by using classless inter-domain routing (CIDR) notation: 192.168.0.0/24, click OK, and then click Next.  9. On the Authentication Method page, select Advanced, and then click Customize.  10. Under First authentication methods, click Add.  11. On the Add First Authentication Methods page, select Preshared key, type TunnelPassword123 in the text box, click OK two times, and then click Next.  Caution  Do not use preshared keys in a production environment. They are not considered secure, and are not easily managed. Use computer certificates either purchased from a third-party vendor, or created by an in-house certification authority, such as a computer that is running Windows Server 2008 R2 with the Active Directory Certificate Services server role. The Preshared key authentication method is used in this guide only because it is beyond the scope of the guide to create a certification authority for this one step.  12. On the Profile page, click Next.  13. On the Name page, type Tunnel on Client, and then click Finish. |

To create the tunnel mode rule on MBRSVR1

|  |
| --- |
| 1. On MBRSVR1, start the Windows Firewall with Advanced Security MMC snap-in.  2. Right-click Connection Security Rules, and then click New Rule.  3. On the Rule Type page, select Tunnel, and then click Next.  4. On the Tunnel Type page, select Gateway-to-client, and then click Next.  5. On the Requirements page, select Require authentication for inbound and outbound connections, and then click Next.  6. On the Tunnel Endpoints (Gateway-to-Client) page, in What are the local endpoints, click Add. Type the subnet identifier for the private network behind the gateway by using classless inter-domain routing (CIDR) notation: 192.168.0.0/24.  7. Under Local tunnel endpoint, type the IPv4 address of the public network connection on MBRSVR1, 131.107.0.100, and then click Next.  Note that you do not have to specify the client IP address; it is already configured as Any IP address. This is a new feature of Windows 7 and Windows Server 2008 R2 that simplifies GPO deployment, because this rule matches all clients of the gateway server. You no longer have to deploy multiple rules with specific local tunnel endpoint settings for each client computer.  Also note the Apply IPsec tunnel authorization check box. This is a feature new of Windows 7 and Windows Server 2008 R2, and appears on Gateway-to-Client and Custom tunnel rule types. On the Properties page of Windows Firewall with Advanced Security, on the IPsec Settings tab, you can specify users and computers that are authorized to connect to this gateway by using the tunnel. Then you can use this check box to specify whether the tunnel established by this rule is subject to those user and computer restrictions. If you use this option then the authentication type you specify on the next page must include support for the credential types that can identify the user or computer accounts authorized.  8. On the Authentication Method page, select Advanced, and then click Customize.  9. Under First authentication methods, click Add.  10. On the Add First Authentication Methods page, select Preshared key, type TunnelPassword123 in the text box, click OK two times, and then click Next.  Caution  Do not use preshared keys in a production environment. They are not considered secure, and are not easily managed. Use computer certificates either purchased from a third-party vendor, or created by an in-house certification authority, such as a computer that is running Windows Server 2008 R2 with the Active Directory Certificate Services server role. The Preshared key authentication method is used in this guide only because it is beyond the scope of the guide to create a certification authority for this one step.  11. On the Profile page, click Next.  12. On the Name page, type Tunnel on Gateway, and then click Finish. |

Next topic: [Step 3: Test Your Tunnel Mode Rules](#z68212fa516504a9ab28198a0f2df7ac5)

Step 3: Test Your Tunnel Mode Rules

With the tunnel mode rules defined, you can now try to access your domain controller through the member server from the client on the public network.

Important

This section of the guide uses features that are present only on computers that are running Windows 7 and Windows Server 2008 R2, and will not work as written on computers that are running earlier versions of Windows.

To communicate with the private network through the tunnel

|  |
| --- |
| 1. On CLIENT1, start the Windows Firewall with Advanced Security MMC snap-in.  2. Expand Monitoring, expand Security Associations, and then click Quick Mode. The list of quick mode security associations (QMSAs) is empty, unless you tried to communicate with the private network.  3. Open a command prompt, and then position the Command Prompt window and the Windows Firewall with Advanced Security snap-in so that you can see the list of QMSAs and still type in the Command Prompt window.  4. At the command prompt, type the command ping 192.168.0.1. The connection succeeds. The first packet might report a loss because of the delay caused by the IPsec tunnel negotiations.  5. On the Actions pane of the Windows Firewall with Advanced Security snap-in, click Refresh.  The QMSA between the client and the gateway is displayed.  6. At the command prompt, type the command net view \\dc1.  This command uses DNS to look up the name of the computer and uses SMB protocol blocks to request shared folder information from DC1 in its role as a file server. All of these network packets are being sent through the IPsec tunnel between CLIENT1 and MBRSVR1. They are then forwarded on to the private network and sent to their destination in plain text. Responses from DC1 are sent to its default gateway, where the tunnel mode rule causes them to be encapsulated in an IPsec ESP header and forwarded to the other network and received by CLIENT1. IPsec on CLIENT1 removes the IPsec ESP header because it is the end of the tunnel, and passes the datagram on to the application that requested it. |

Next topic: [Summary](#z917f57d811774da4aa754e08d94f5876)

Summary

Windows Firewall with Advanced Security is an important element in a defense-in-depth security strategy to help secure the computers in your organization, and help mitigate threats that either bypass your perimeter firewall or originate from within the network.

In this guide, you were introduced to the features of the Windows Firewall with Advanced Security included with Windows 7, Windows Vista, Windows Server 2008 R2, and Windows Server 2008:

 You used Windows Firewall with Advanced Security to set up basic inbound and outbound firewall rules.

 You created Group Policy objects that configure firewall settings on all the computers in a domain, and ensured that users cannot override those settings.

 You created a set of basic domain isolation rules that restrict domain-member computers from accepting network traffic from computers that are not members of the domain.

 You created connection security rules that isolate servers which store sensitive information, by restricting access to only computers that are members of approved groups.

 You created firewall rules that enabled specific trusted computers to bypass firewall requirements.

 Finally, you created tunnel mode connection security rules that caused network traffic destined for a certain network address to be protected by IPsec and then routed to a gateway server where it the packet is extracted and then forwarded to the destination computer.

We hope you found this document helpful. Your feedback is valuable and welcome! Please send your comments and suggestions to [Windows Firewall with Advanced Security Documentation Feedback](mailto://wfasdoc@microsoft.com?subject=Feedback%20on%20IPsec%20and%20Firewall%20Documentation%20–%20WFAS%20SxS%20Deploying%20FW%20and%20IPsec%20Policies%20Guide&body=I%20want%20to%20provide%20the%20following%20feedback%20on%20the%20document%20Step-by-Step%20Guide:%20Deploying%20Windows%20Firewall%20and%20IPsec%20Policies.%0A%0A) (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.

Next topic: [Additional References](#ze4248de52d0747219c54163e351e33fb)

Additional References

For more information about the technologies discussed in this guide, see the following locations.

Windows Firewall with Advanced Security

 Windows Firewall (<http://go.microsoft.com/fwlink/?linkid=95393>)

This page contains links to the documentation currently available for Windows Firewall, for both the version available on Windows XP with Service Pack 2 (SP2) or later and Windows Server 2003, and the version available on Windows 7, Windows Vista, Windows Server 2008 R2, and Windows Server 2008.

 Windows Firewall with Advanced Security - Diagnostics and Troubleshooting (<http://go.microsoft.com/fwlink/?linkid=95372>)

This article describes how Windows Firewall with Advanced Security works, what the common troubleshooting situations are, and which tools you can use for troubleshooting.

IPsec

 IPsec (<http://go.microsoft.com/fwlink/?linkid=95394>)

This page contains links to the documentation currently available for Internet Protocol security (IPsec), for both the version available on Windows XP and Windows Server 2003, and the version available as connection security rules in Windows Firewall with Advanced Security on Windows 7, Windows Vista, Windows Server 2008 R2, and Windows Server 2008.

 Simplifying IPsec Policy with the Simple Policy Update (<http://go.microsoft.com/fwlink/?linkid=94767>)

This article describes a downloadable update available for Windows XP with SP2 and Windows Server 2003 with Service Pack 1 (SP1). (The update is built into Windows XP with SP3 and Windows Server 2003 Service Pack 2). The update changes the behavior of IPsec negotiation so that the IPsec policy rules can be simplified, in some cases significantly reducing the number of required IP filters and their ongoing maintenance.

Server and Domain Isolation

 Server and Domain Isolation (<http://go.microsoft.com/fwlink/?linkid=95395>)

This page contains links to documentation that support the most common uses for IPsec: server and domain isolation.

Group Policy

 Group Policy (<http://go.microsoft.com/fwlink/?linkid=93542>)

This page contains links to the documentation currently available for Group Policy.

 HOWTO: Leverage Group Policies with WMI Filters (<http://go.microsoft.com/fwlink/?linkid=93760>)

This article describes how to create a WMI filter to set the scope of a GPO based on computer attributes, such as operating system version number.