Windows Server® 2008

Windows Firewall with Advanced Security Design Guide

Microsoft Corporation

Published: March 2008

Author: Dave Bishop

Editor: Scott Somohano

Reviewers: Sarah Wahlert, Jason Popp, Jorge Coronel Mendoza

Abstract

This guide helps you design Windows Firewall with Advanced Security settings and rules that meet your goals for network security. Use this guide together with the Windows Firewall with Advanced Security Deployment Guide during your planning stages. The Design Guide answers the "what," "why," and "when" questions before you work on the "how" questions answered in the Deployment Guide.

Microsoft®

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

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

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.

Contents

Windows Firewall with Advanced Security Design Guide

Windows Firewall with Advanced Security in Windows Vista® and Windows Server® 2008 is a host firewall that helps secure the computer in two ways. First, it can filter the network traffic permitted to enter the computer from the network, and also control what network traffic the computer is allowed to send to the network. Second, Windows Firewall with Advanced Security supports IPsec, which enables you to require authentication from any computer that is attempting to communicate with your computer. When authentication is required, computers that cannot authenticate cannot communicate with your computer. By using IPsec, you can also require that specific network traffic be encrypted to prevent it from being read or intercepted while in transit between computers.

The interface for Windows Firewall with Advanced Security is much more capable and flexible than the consumer-friendly interface found in the Windows Firewall Control Panel. They both interact with the same underlying services, but provide different levels of control over those services. While the Windows Firewall Control Panel meets the needs for protecting a single computer in a home environment, it does not provide enough centralized management or security features to help secure more complex network traffic found in a typical business enterprise environment.

Tip

> If you are reading this guide on the Web in the Windows Server Technical Library, then click the **sync toc** at the top of the navigation pane, and then expand the node for Windows Firewall with Advanced Security. You can view any topic in the guide by clicking its name in the navigation pane.

For more overview information about Windows Firewall with Advanced Security and its common uses, see the following topics on the Microsoft Web site:

- Getting Started with Windows Firewall with Advanced Security

  http://go.microsoft.com/fwlink/?linkid=64343

- Introduction to Server and Domain Isolation

  http://go.microsoft.com/fwlink/?linkid=94632

For the complete list of documentation for Windows Firewall with Advanced Security, see the Windows Firewall with Advanced Security Content Roadmap at http://go.microsoft.com/fwlink/?LinkID=64342.

About this guide

This guide provides recommendations to help you to choose or create a design for deploying Windows Firewall with Advanced Security in your enterprise environment. The guide describes some of the common goals for using Windows Firewall with Advanced Security, and then helps you map the goals that apply to your scenario to the designs that are presented in this guide.

This guide is intended for the IT professional who has been assigned the task of deploying firewall and IPsec technologies on an organization's network to help meet the organization's security goals.

Windows Firewall with Advanced Security should be part of a comprehensive security solution that implements a variety of security technologies, such as perimeter firewalls, intrusion detection systems, virtual private networking (VPN), IEEE 802.1X authentication for wireless and wired connections, and IPsec connection security rules.

To successfully use this guide, you need a good understanding of both the capabilities provided by Windows Firewall with Advanced Security, and how to deliver configuration settings to your managed computers by using Group Policy in Active Directory.

You can use the deployment goals to form one of these Windows Firewall with Advanced Security designs, or a custom design that combines elements from those presented here:

- **Basic firewall policy design**. Restricts network traffic in and out of your computers to only that which is needed and authorized.
- **Domain isolation policy design**. Prevents computers that are domain members from receiving unsolicited network traffic from computers that are not domain members. Additional "zones" can be established to support the special requirements of some computers, such as:
    - A "boundary zone" for computers that must be able to receive requests from non-isolated computers.
    - An "encryption zone" for computers that store sensitive data that must be protected during network transmission.
- **Server isolation policy design**. Restricts access to a server to only a limited group of authorized users and computers. Commonly configured as a zone in a domain isolation design, but can also be configured as a stand-alone design, providing many of the benefits of domain isolation to a small set of computers.
- **Certificate-based isolation policy design**. This design is a complement to either of the previous two designs, and supports any of their capabilities. It uses cryptographic certificates that are deployed to clients and servers for authentication, instead of the Kerberos V5 authentication used by default in Active Directory. This enables computers that are not part of an Active Directory domain, such as computers running operating systems other than Windows, to participate in your isolation solution.

In addition to descriptions and example for each design, you will find guidelines for gathering required data about your environment. You can then use these guidelines to plan and design your Windows Firewall with Advanced Security deployment. After you read this guide, and finish gathering, documenting, and mapping your organization's requirements, you have the information that you need to begin deploying Windows Firewall with Advanced Security using the guidance in the Windows Firewall with Advanced Security Deployment Guide.

You can find the Windows Firewall with Advanced Security Deployment Guide at these locations:

- http://go.microsoft.com/fwlink/?linkid=102569 (Web page)
- http://go.microsoft.com/fwlink/?linkid=102571 (Downloadable Word document)

Terminology used in this guide

The following table identifies and defines terms used throughout this guide.

Term	Definition
Active Directory domain	A group of computers and users managed by an administrator by using Active Directory Domain Services (AD DS). Computers in a domain share a common directory database and security policies. Multiple domains can co-exist in a "forest," with trust relationships that establish the forest as the security boundary.
Authentication	A process that enables the sender of a message to prove its identity to the receiver. For connection security in Windows, authentication is implemented by the IPsec protocol suite.
Boundary zone	A subset of the computers in an isolated domain that must be able to receive unsolicited and non-authenticated network traffic from computers that are not members of the isolated domain. Computers in the boundary zone request but do not require authentication. They use IPsec to communicate with other computers in the isolated domain.
Connection security rule	A rule in Windows Firewall with Advanced Security that contains a set of conditions and an action to be applied to network packets that match the conditions. The action can allow the packet, block the packet, or require the packet to be protected by IPsec. In previous versions of Windows, this was called an *IPsec rule*.
Certificate-based isolation	A way to add computers that cannot use Kerberos V5 authentication to an isolated domain, by using an alternate authentication technique. Every computer in the isolated domain and the computers that cannot use Kerberos V5 are provided with a computer certificate that can be used to authenticate with

Term	Definition
	each other. Certificate-based isolation requires a way to create and distribute an appropriate certificate (if you choose not to purchase one from a commercial certificate provider).
Domain isolation	A technique for helping protect the computers in an organization by requiring that the computers authenticate each other's identity before exchanging information, and refusing connection requests from computers that cannot authenticate. Domain isolation takes advantage of Active Directory domain membership and the Kerberos V5 authentication protocol available to all members of the domain. Also see "Isolated domain" in this table.
Encryption zone	A subset of the computers in an isolated domain that process sensitive data. Computers that are part of the encryption zone have all network traffic encrypted to prevent viewing by non-authorized users. Computers that are part of the encryption zone also typically are subject to the access control restrictions of server isolation.
Firewall rule	A rule in Windows Firewall with Advanced Security that contains a set of conditions used to determine whether a network packet is allowed to pass through the firewall. By default, the firewall rules in Windows Vista and Windows Server 2008 block unsolicited inbound network traffic. Likewise, by default, all outbound network traffic is allowed. The firewall included in previous versions of Windows only filtered inbound network traffic.
Internet Protocol security (IPsec)	A set of industry-standard, cryptography-based protection services and protocols. IPSec protects all protocols in the TCP/IP protocol suite except Address Resolution Protocol (ARP).
IPsec policy	A collection of connection security rules that provide the required protection to network traffic entering and leaving the computer. The

Term	Definition
	protection includes authentication of both the sending and receiving computer, integrity protection of the network traffic exchanged between them, and can include encryption.
Isolated domain	An Active Directory domain (or an Active Directory forest, or set of domains with two-way trust relationships) that has Group Policy settings applied to help protect its member computers by using IPsec connection security rules. Members of the isolated domain require authentication on all unsolicited inbound connections (with exceptions handled by the other zones). In this guide, the term *isolated domain* refers to the IPsec concept of a group of computers that can share authentication. The term *Active Directory domain* refers to the group of computers that share a security database by using Active Directory.
Server isolation	A technique for using group membership to restrict access to a server that is typically already a member of an isolated domain. The additional protection comes from using the authentication credentials of the requesting computer to determine its group membership, and then only allowing access if the computer account (and optionally the user account) is a member of an authorized group.
Solicited network traffic	Network traffic that is sent in response to a request. By default, Windows Firewall with Advanced Security allows all solicited network traffic through.
Unsolicited network traffic	Network traffic that is not a response to an earlier request, and that the receiving computer cannot necessarily anticipate. By default, Windows Firewall with Advanced Security blocks all unsolicited network traffic.
Zone	A zone is a logical grouping of computers that share common IPsec policies because of their communications requirements. For example,

Term	Definition
	the boundary zone permits inbound connections from non-trusted computers. The encryption zone requires that all connections be encrypted. This is not related to the term zone as used by Domain Name System (DNS).

Next: Understanding the Windows Firewall with Advanced Security Design Process

Understanding the Windows Firewall with Advanced Security Design Process

Designing any deployment starts by performing several important tasks:

- Identifying Your Windows Firewall with Advanced Security Deployment Goals
- Mapping Your Deployment Goals to a Windows Firewall with Advanced Security Design
- Evaluating Windows Firewall with Advanced Security Design Examples

After you identify your deployment goals and map them to a Windows Firewall with Advanced Security design, you can begin documenting the design based on the processes that are described in the following topics:

- Designing a Windows Firewall with Advanced Security Strategy
- Planning Your Windows Firewall with Advanced Security Design

Next: Identifying Your Windows Firewall with Advanced Security Deployment Goals

Identifying Your Windows Firewall with Advanced Security Deployment Goals

Correctly identifying your Windows Firewall with Advanced Security deployment goals is essential for the success of your Windows Firewall with Advanced Security design project. Form a project team that can clearly articulate deployment issues in a vision statement. When you write your vision statement, identify, clarify, and refine your deployment goals. Prioritize and, if possible, combine your deployment goals so that you can design and deploy Windows Firewall with Advanced Security by using an iterative approach. You can take advantage of the predefined Windows Firewall with Advanced Security deployment goals presented in this guide that are relevant to your scenarios.

The following table lists the three main tasks for articulating, refining, and subsequently documenting your Windows Firewall with Advanced Security deployment goals.

Deployment goal tasks	Reference links
Evaluate predefined Windows Firewall with	Predefined deployment goals:

Deployment goal tasks	Reference links
Advanced Security deployment goals that are provided in this section of the guide, and combine one or more goals to reach your organizational objectives.	• Protect Computers from Unwanted Network Traffic • Restrict Access to Only Trusted Computers • Require Encryption When Accessing Sensitive Network Resources • Restrict Access to Only Specified Users or Computers
Map one goal or a combination of the predefined deployment goals to an existing Windows Firewall with Advanced Security design.	• Mapping Your Deployment Goals to a Windows Firewall with Advanced Security Design
Based on the status of your current infrastructure, document your deployment goals for your Windows Firewall with Advanced Security design into a deployment plan.	• Designing a Windows Firewall with Advanced Security Strategy • Planning Your Windows Firewall with Advanced Security Design

Next: Protect Computers from Unwanted Network Traffic

Protect Computers from Unwanted Network Traffic

Although network perimeter firewalls provide important protection to network resources from external threats, there are network threats that a perimeter firewall cannot protect against. Some attacks might successfully penetrate the perimeter firewall, and at that point what can stop it? Other attacks might originate from inside the network, such as a computer virus that is brought in on portable media and run on a trusted computer. Portable computers are often taken outside the network and connected directly to the Internet, without adequate protection between the computer and security threats.

Running a host-based firewall on every computer that your organization manages is an important layer in a "defense-in-depth" security strategy. A host-based firewall can help protect against attacks that originate from inside the network and also provide additional protection against attacks from outside the network that manage to penetrate the perimeter firewall. It also travels with a portable computer to provide protection when it is away from the organization's network.

A host-based firewall helps secure a computer by dropping all network traffic that does not match the administrator-designed rule set for permitted network traffic. This design, which corresponds to Basic Firewall Policy Design, provides the following benefits:

- Network traffic that is a reply to a request from the local computer is permitted into the computer from the network.

- Network traffic that is unsolicited, but that matches a rule for allowed network traffic, is permitted into the computer from the network.

For example, Woodgrove Bank wants a computer that is running SQL Server to be able to receive the SQL queries sent to it by client computers. The firewall policy deployed to the computer that is running SQL Server includes firewall rules that specifically allow inbound network traffic for the SQL Server program.

- Outbound network traffic that is not specifically blocked is allowed on the network.

For example, Woodgrove Bank has a corporate policy that prohibits the use of certain peer-to-peer file sharing programs. The firewall policy deployed to the computers on the network includes firewall rules that block both inbound and outbound network traffic for the prohibited programs. All other outbound traffic is permitted.

The following component is recommended for this deployment goal:

- **Active Directory**: Active Directory supports centralized management of connection security rules by configuring the rules in one or more Group Policy objects (GPOs) that can be automatically applied to all relevant computers in the domain. For more information about Active Directory, see Additional Resources.

Other means of deploying a firewall policy are available, such as creating scripts that use the **netsh** command-line tool, and then running those scripts on each computer in the organization. This guide uses Active Directory as a recommended means of deployment because of its ability to scale to very large organizations.

Next: Restrict Access to Only Trusted Computers

Restrict Access to Only Trusted Computers

Your organizational network likely has a connection to the Internet. You also likely have partners, vendors, or contractors who attach computers that are not owned by your organization to your network. Because you do not manage those computers, you cannot trust them to be free of malicious software, maintained with the latest security updates, or in any way in compliance with your organization's security policies. These untrustworthy computers both on and outside of your physical network must not be permitted to access your organization's computers except where it is truly required.

To mitigate this risk, you must be able to isolate the computers you trust, and restrict their ability to receive unsolicited network traffic from untrusted computers. By using connection security and firewall rules available in Windows Firewall with Advanced Security, you can logically isolate the computers that you trust by requiring that all unsolicited inbound network traffic be authenticated. Authentication ensures that each computer or user can positively identify itself by using credentials that are trusted by the other computer. Connection security rules can be configured to use IPsec with the Kerberos V5 protocol available in Active Directory, or certificates issued by a trusted certification authority as the authentication method.

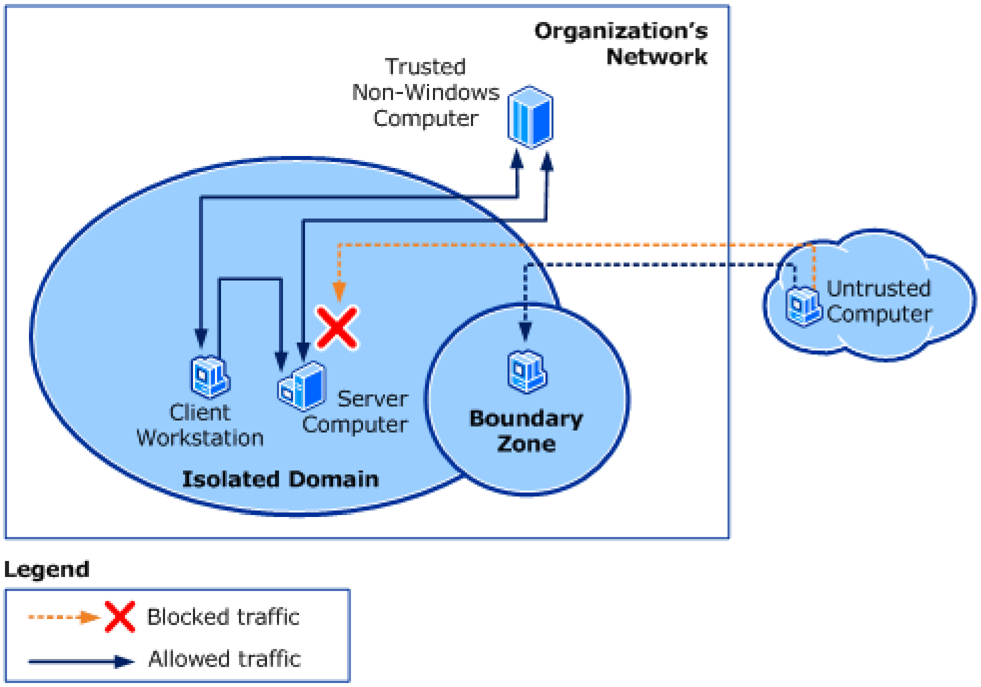
Note

Because the primary authentication method recommended for computers that are running Windows is to use the Kerberos V5 protocol with membership in an Active

Directory domain, this guide refers to this logical separation of computers as *domain isolation*, even when certificates are used to extend the protection to computers that are not part of an Active Directory domain.

The protection provided by domain isolation can help you comply with regulatory and legislative requirements, such as those found in the Federal Information Security Management Act of 2002 (FISMA), the Sarbanes-Oxley Act of 2002, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and other government and industry regulations.

The following illustration shows an isolated domain, with one of the zones that are optionally part of the design. The rules that implement both the isolated domain and the different zones are deployed by using Group Policy and Active Directory.



These goals, which correspond to Domain Isolation Policy Design and Certificate-based Isolation Policy Design, provide the following benefits:

- Computers in the isolated domain accept unsolicited inbound network traffic only when it can be authenticated as coming from another computer in the isolated domain. Exemption rules can be defined to allow inbound traffic from trusted computers that for some reason cannot perform IPsec authentication.

For example, Woodgrove Bank wants all of its computers to block all unsolicited inbound network traffic from any computer that it does not manage. The connection security rules deployed to domain member computers require authentication as a domain member or by using a certificate before an unsolicited inbound network packet is accepted.

- Computers in the isolated domain can still send outbound network traffic to untrusted computers and receive the responses to the outbound requests.

For example, Woodgrove Bank wants its users at client computers to be able to access Web sites on the Internet. The default Windows Firewall with Advanced Security settings for outbound network traffic allow this. No additional rules are required.

These goals also support optional zones that can be created to add customized protection to meet the needs of subsets of an organization's computers:

- Computers in the "boundary zone" are configured to use connection security rules that request but do not require authentication. This enables them to receive unsolicited inbound network traffic from untrusted computers, and also to receive traffic from the other members of the isolated domain.

For example, Woodgrove Bank has a server that must be accessed by its partners' computers through the Internet. The rules applied to computers in the boundary zone use authentication when the client computer can support it, but do not block the connection if the client computer cannot authenticate.

- Computers in the "encryption zone" require that all network traffic in and out must be encrypted to secure potentially sensitive material when it is sent over the network.

For example, Woodgrove Bank wants the computers running SQL Server to only transmit data that is encrypted to help protect the sensitive data stored on those computers.

The following components are required for this deployment goal:

- **Active Directory**: Active Directory supports centralized management of connection security rules by configuring the rules in one or more GPOs that can be automatically applied to all relevant computers in the domain. For more information about Active Directory, see Additional Resources.

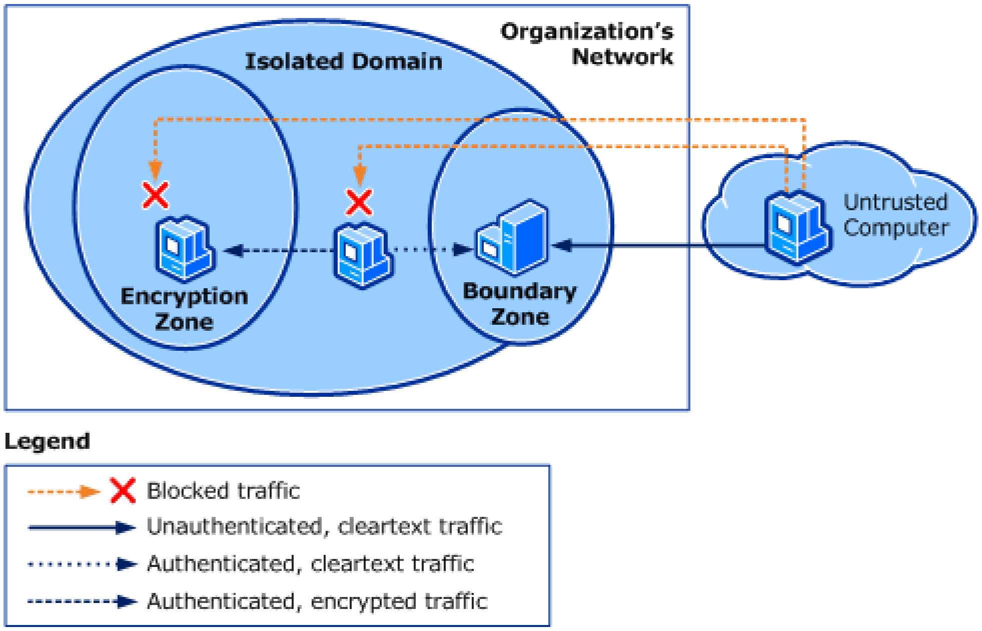
Next: Require Encryption When Accessing Sensitive Network Resources

Require Encryption When Accessing Sensitive Network Resources

The use of authentication in the previously described goal (Restrict Access to Only Trusted Computers) enables a computer in the isolated domain to block traffic from untrusted computers. However, it does not prevent an untrusted computer from eavesdropping on the network traffic shared between two trusted computers, because network packets are not encrypted by default.

For computers that share sensitive information over the network, Windows Firewall with Advanced Security enables you to specify that all such network traffic must be encrypted. Using encryption can help you comply with regulatory and legislative requirements such as those found in the Federal Information Security Management Act of 2002 (FISMA), the Sarbanes-Oxley Act of 2002, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and other government and industry regulations. By creating connection security rules that apply to computers that host and exchange sensitive data, you can help protect the confidentiality of that data by encrypting it.

The following illustration shows an encryption zone in an isolated domain. The rules that implement both the isolated domain and the different zones are deployed by using Group Policy and Active Directory.



This goal provides the following benefits:

- Computers in the encryption zone require authentication to communicate with other computers. This works no differently from the domain isolation goal and design. For more information, see Restrict Access to Only Trusted Computers.
- Computers in the encryption zone require that all inbound and outbound network traffic be encrypted.

For example, Woodgrove Bank processes sensitive customer data on a computer that must be protected from eavesdropping by computers on the network. Connection security rules specify that all traffic must be encrypted by a sufficiently complex encryption algorithm to help protect the data.

- Computers in the encryption zone are often good candidates for server isolation, where access is limited to only computer accounts and user accounts that are members of an authorized access group. In many organizations, the encryption zone and the server isolation zone are one and the same. For more information, see Restrict Access to Only Specified Users or Computers.

The following components are required for this deployment goal:

- **Active Directory**: Active Directory supports centralized management of connection security rules by configuring the rules in one or more GPOs that can be automatically applied to all relevant computers in the domain. For more information about Active Directory, see Additional Resources.

Next: Restrict Access to Only Specified Users or Computers

Restrict Access to Only Specified Users or Computers

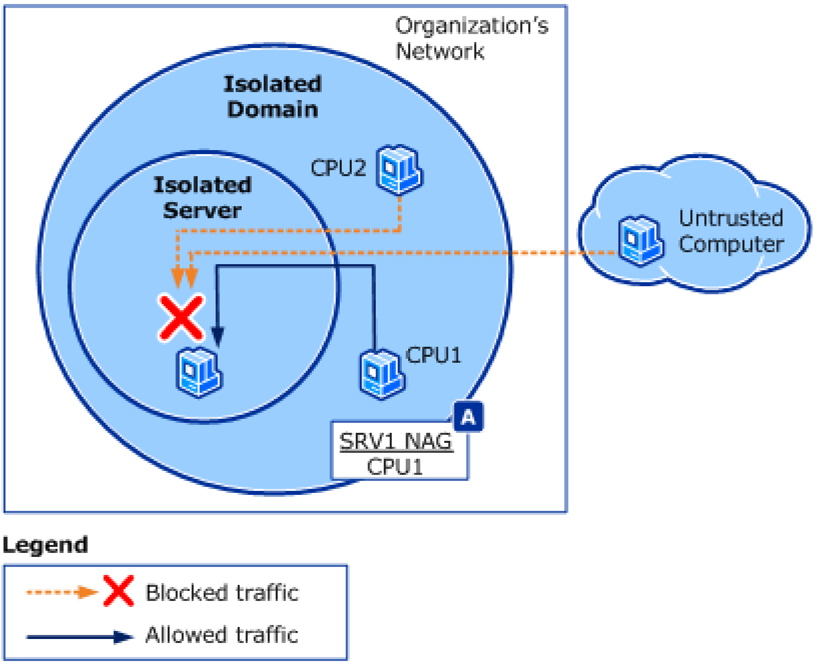
Domain isolation (as described in the previous goal Restrict Access to Only Trusted Computers) prevents computers that are members of the isolated domain from accepting network traffic from untrusted computers. However, some computers on the network might host sensitive data that must be additionally restricted to only those users and computers that have a business requirement to access the data.

Windows Firewall with Advanced Security enables you to restrict access to computers and users that are members of domain groups authorized to access that computer. These groups are called *network access groups (NAGs)*. When a computer authenticates to a server, the server checks the group membership of the computer account and the user account, and grants access only if membership in the NAG is confirmed. Adding this check creates a virtual "secure zone" within the domain isolation zone. You can have multiple computers in a single secure zone, and it is likely that you will create a separate zone for each set of servers that have specific security access needs. Computers that are part of this server isolation zone are often also part of the encryption zone (see Require Encryption When Accessing Sensitive Network Resources).

Restricting access to only users and computers that have a business requirement can help you comply with regulatory and legislative requirements, such as those found in the Federal Information Security Management Act of 2002 (FISMA), the Sarbanes-Oxley Act of 2002, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and other government and industry regulations.

Windows Vista and Windows Server 2008 enable you to restrict access by specifying either computer or user credentials. Windows XP and Windows Server 2003 do not support user-based authentication, but a similar behavior can be achieved by denying the "Access this computer from the network" user right to all users except members of the NAG.

The following illustration shows an isolated server, and examples of computers that can and cannot communicate with it. Computers that are outside the Woodgrove corporate network, or computers that are in the isolated domain but are not members of the required NAG, cannot communicate with the isolated server.



This goal, which corresponds to Server Isolation Policy Design, provides the following features:

- Isolated servers accept unsolicited inbound network traffic only from computers or users that are members of the NAG.
- Isolated servers can be implemented as part of an isolated domain, and treated as another zone. Members of the zone group receive a GPO with rules that require authentication, and that specify that only network traffic authenticated as coming from a member of the NAG is allowed.
- Server isolation can also be configured independently of an isolated domain. To do so, configure only the computers that must communicate with the isolated server with connection security rules to implement authentication and check NAG membership.
- A server isolation zone can be simultaneously configured as an encryption zone. To do this, configure the GPO with rules that force encryption in addition to requiring authentication and restricting access to NAG members. For more information, see Require Encryption When Accessing Sensitive Network Resources.

The following components are required for this deployment goal:

- **Active Directory**: Active Directory supports centralized management of connection security rules by configuring the rules in one or more GPOs that can be automatically applied to all relevant computers in the domain. For more information about Active Directory, see Additional Resources.

Next: Mapping Your Deployment Goals to a Windows Firewall with Advanced Security Design

Mapping Your Deployment Goals to a Windows Firewall with Advanced Security Design

After you finish reviewing the existing Windows Firewall with Advanced Security deployment goals and you determine which goals are important to your specific deployment, you can map those goals to a specific Windows Firewall with Advanced Security design.

Important

> The first three designs presented in this guide build on each other to progress from simpler to more complex. Therefore during deployment, consider implementing them in the order presented. Each deployed design also provides a stable position from which to evaluate your progress, and to make sure that your goals are being met before you continue to the next design.

Use the following table to determine which Windows Firewall with Advanced Security design maps to the appropriate combination of Windows Firewall with Advanced Security deployment goals for your organization. This table refers only to the Windows Firewall with Advanced Security designs as described in this guide. However, you can create a hybrid or custom Windows Firewall with Advanced Security design by using any combination of the Windows Firewall with Advanced Security deployment goals to meet the needs of your organization.

Deployment Goals	Basic Firewall Policy Design	Domain Isolation Policy Design	Server Isolation Policy Design	Certificate-based Isolation Policy Design
Protect Computers from Unwanted Network Traffic	Yes	Yes	Yes	Yes
Restrict Access to Only Trusted Computers	-	Yes	Yes	Yes
Restrict Access to Only Specified Users or Computers	-	-	Yes	Yes
Require Encryption When Accessing Sensitive Network Resources	-	Optional	Optional	Optional

To examine details for a specific design, click the design title at the top of the column in the preceding table.

Next: Basic Firewall Policy Design

Basic Firewall Policy Design

Many organizations have a network perimeter firewall that is designed to prevent the entry of malicious traffic in to the organization's network, but do not have a host-based firewall enabled on each computer in the organization.

The basic firewall policy design helps you to protect the computers in your organization from unwanted network traffic that gets through the perimeter defenses, or that originates from inside your network. In this design, you deploy firewall rules to each computer in your organization to allow traffic that is required by the programs that are used. Traffic that does not match the rules is dropped.

Traffic can be blocked or permitted based on the characteristics of each network packet: its source or destination IP address, its source or destination port numbers, the program on the computer that receives the inbound packet, and so on. This design can also be deployed together with one or more of the other designs that add IPsec protection to the network traffic permitted.

Many network administrators do not want to tackle the difficult task of determining all the appropriate rules for every program that is used by the organization, and then maintaining that list over time. In fact, most programs do not require specific firewall rules. The default behavior of Windows and most contemporary applications makes this task easy:

- On client computers, the default firewall behavior already supports typical client programs. Programs designed for Windows Vista and Windows Server 2008 create any required rules for you as part of the installation process. You only have to create a rule if the client program must be able to receive unsolicited inbound network traffic from another computer.
- When you install a server program that must accept unsolicited inbound network traffic, the installation program likely creates or enables the appropriate rules on the server for you.

  For example, when you install a server role by using the Role Management Tool in Windows Server 2008, the appropriate firewall rules are created and enabled automatically. For both Windows Server 2003 and Windows Server 2008, the Security Configuration Wizard configures firewall rules appropriate for the programs and services installed on the server.
- For other standard network behavior, the predefined rules that are built into Windows Vista and Windows Server 2008 can easily be configured in a GPO and deployed to the computers in your organization.

  For example, by using the predefined groups for Core Networking and File and Printer Sharing you can easily configure GPOs with rules for those frequently used networking protocols.

With few exceptions, the firewall can be enabled on all configurations of Windows Vista or Windows Server 2008. Therefore, we recommended that you enable the firewall on every computer in your organization. This includes servers in your perimeter network, on mobile and remote clients that connect to the network, and on all servers and clients in your internal network.

Caution

- **Stopping the service associated with Windows Firewall with Advanced Security is not supported by Microsoft**.
- By default, in new installations, Windows Firewall is turned on in both Windows Vista and Windows Server 2008. If you must disable the firewall, such as when you want to use a third-party firewall program, do not disable Windows Firewall by stopping the service. Instead, use the Windows Firewall with Advanced Security interface (or equivalent Group Policy setting) to turn the firewall off.
- If you turn off the Windows Firewall with Advanced Security service you lose other benefits provided by the service, such as the ability to use IPsec connection security rules, Windows Service Hardening, and network protection from forms of attacks that use network fingerprinting. For more information about Windows Service Hardening, see http://go.microsoft.com/fwlink/?linkid=104976.
- Third-party firewall software that is compatible with Windows Vista and Windows Server 2008 can programmatically disable only the parts of Windows Firewall with Advanced Security that might need to be disabled for compatibility. Do not disable the firewall yourself for this purpose.

An organization typically uses this design as a first step toward a more comprehensive Windows Firewall with Advanced Security design that adds server isolation and domain isolation.

After implementing this design, your administrative team will have centralized management of the firewall rules applied to all computers that are running Windows in your organization.

Important

If you also intend to deploy the Domain Isolation Policy Design, or the Server Isolation Policy Design, we recommend that you do the design work for all three designs together, and then deploy in layers that correspond with each design.

The basic firewall design can be applied to computers that are part of an Active Directory forest. Active Directory is required to provide the centralized management and deployment of Group Policy objects that contain the firewall settings and rules.

For more information about this design:

- This design coincides with the deployment goal to Protect Computers from Unwanted Network Traffic.
- To learn more about this design, see Firewall Policy Design Example.
- Before completing the design, gather the information described in Designing a Windows Firewall with Advanced Security Strategy.
- To help you make the decisions required in this design, see Planning Settings for a Basic Firewall Policy.
- For a list of detailed tasks that you can use to deploy your basic firewall policy design, see "Checklist: Implementing a Basic Firewall Policy Design" in the Windows Firewall with Advanced Security Deployment Guide at http://go.microsoft.com/fwlink/?linkid=98308.

Next: Domain Isolation Policy Design

Domain Isolation Policy Design

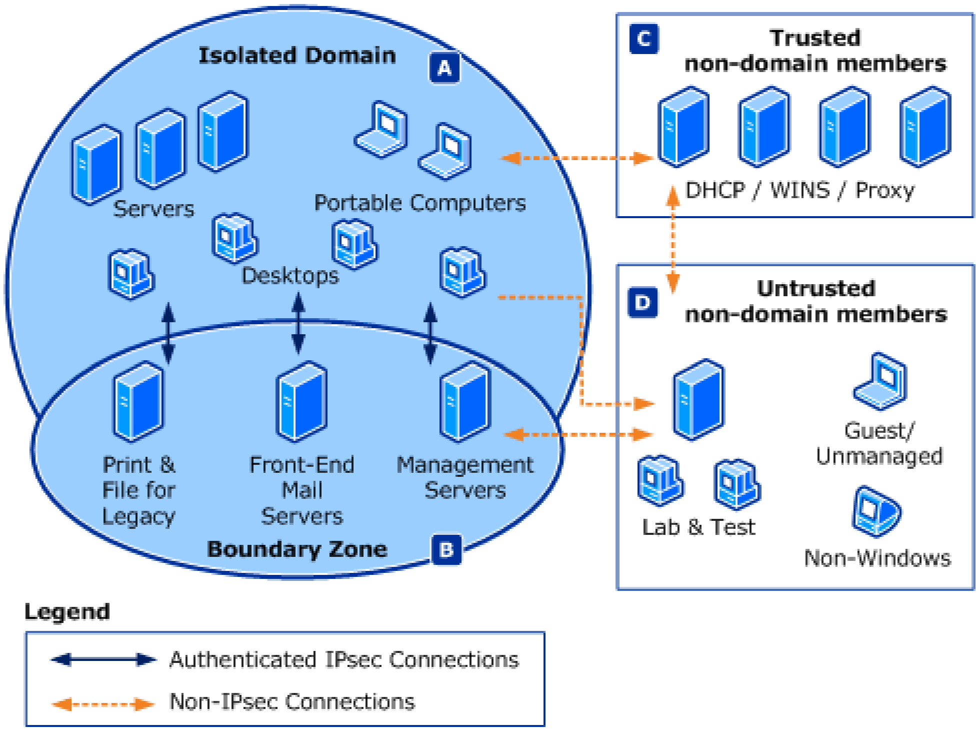
In the domain isolation policy design, you configure the computers on your network to accept only connections coming from computers that are authenticated as members of the same isolated domain.

This design typically begins with a network configured as described in the Basic Firewall Policy Design section. For this design, you then add connection security and IPsec rules to configure computers in the isolated domain to accept only network traffic from other computers that can authenticate as a member of the isolated domain. After implementing the new rules, your computers reject unsolicited network traffic from computers that are not members of the isolated domain.

The isolated domain might not be a single Active Directory domain. It can consist of all the domains in a forest, or domains in separate forests that have two-way trust relationships configured between them.

By using connection security rules based on IPsec, you provide a logical barrier between computers even if they are connected to the same physical network segment.

The design is shown in the following illustration, with the arrows that show the permitted communication paths.



Characteristics of this design, as shown in the diagram, include the following:

- Isolated domain (area A) - Computers in the isolated domain receive unsolicited inbound traffic only from other members of the isolated domain or from computers referenced in authentication exemption rules. Computers in the isolated domain can send traffic to any computer. This includes unauthenticated traffic to computers that are not in the isolated domain. Computers that cannot join an Active Directory domain, but that can use certificates for authentication, can be part of the isolated domain. For more information, see the Certificate-based Isolation Policy Design.

- Boundary zone (area B) - Computers in the boundary zone are part of the isolated domain but are allowed to accept inbound connections from untrusted computers, such as clients on the Internet.

Computers in the boundary zone request but do not require authentication to communicate. When a member of the isolated domain communicates with a boundary zone member the traffic is authenticated. When a computer that is not part of the isolated domain communicates with a boundary zone member the traffic is not authenticated.

Because boundary zone computers are exposed to network traffic from untrusted and potentially hostile computers, they must be carefully managed and secured. Put only the computers that must be accessed by external computers in this zone. Use firewall rules to ensure that network traffic is accepted only for services that you want exposed to non-domain member computers.

- Trusted non-domain members (area C) - Computers on the network that are not domain members or that cannot use IPsec authentication are allowed to communicate by configuring authentication exemption rules. These rules enable computers in the isolated domain to accept inbound connections from these trusted non-domain member computers.
- Untrusted non-domain members (area D) - Computers that are not managed by your organization and have an unknown security configuration must have access only to those computers required for your organization to correctly conduct its business. Domain isolation exists to put a logical barrier between these untrusted computers and your organization's computers.

After implementing this design, your administrative team will have centralized management of the firewall and connection security rules applied to the computers that are running Windows Vista and Windows Server 2008 in your organization.

Important

This design builds on the Basic Firewall Policy Design, and in turn serves as the foundation for the Server Isolation Policy Design. If you plan to deploy all three, we recommend that you do the design work for all three together, and then deploy in the sequence presented.

This design can be applied to computers that are part of an Active Directory forest. Active Directory is required to provide the centralized management and deployment of Group Policy objects that contain the connection security rules.

In order to expand the isolated domain to include computers that cannot be part of an Active Directory domain, see the Certificate-based Isolation Policy Design.

For more information about this design:

- This design coincides with the deployment goals to Protect Computers from Unwanted Network Traffic, Restrict Access to Only Trusted Computers, and optionally Require Encryption When Accessing Sensitive Network Resources.
- To learn more about this design, see the Domain Isolation Policy Design Example.
- Before completing the design, gather the information described in Designing a Windows Firewall with Advanced Security Strategy.
- To help you make the decisions required in this design, see Planning Domain Isolation Zones and Planning Group Policy Deployment for Your Isolation Zones.
- For a list of tasks that you can use to deploy your domain isolation policy design, see "Checklist: Implementing a Domain Isolation Policy Design" in the Windows Firewall with Advanced Security Deployment Guide at http://go.microsoft.com/fwlink/?linkid=98308.

Next: Server Isolation Policy Design

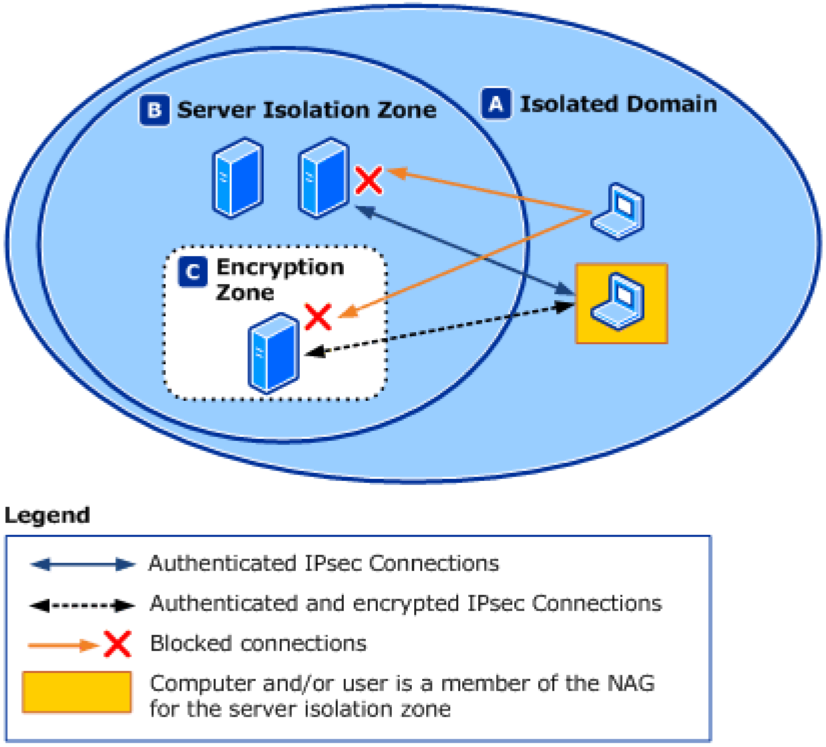
Server Isolation Policy Design

In the server isolation policy design, you assign servers to a zone that allows access only to users and computers that authenticate as members of an approved network access group (NAG).

This design typically begins with a network configured as described in the Domain Isolation Policy Design section. For this design, you then create zones for servers that have additional security requirements. The zones can limit access to the server to only members of authorized groups, and can optionally require the encryption of all traffic in or out of these servers. This can be done on a per server basis, or for a group of servers that share common security requirements.

You can implement a server isolation design without using domain isolation. To do this, you use the same principles as domain isolation, but instead of applying them to an Active Directory domain, you apply them only to the computers that must be able to access the isolated servers. The GPO contains connection security and firewall rules that require authentication when communicating with the isolated servers. In this case, the NAGs that determine which users and computers can access the isolated server are also used to determine which computers receive the GPO.

The design is shown in the following illustration, with arrows that show the permitted communication paths.


B Server Isolation Zone
A Isolated Domain
C Encryption Zone
Legend
Authenticated IPsec Connections
Authenticated and encrypted IPsec Connections
Blocked connections
Computer and/or user is a member of the NAG for the server isolation zone

Characteristics of this design include the following:

- Isolated domain (area A) - The same isolated domain described in the Domain Isolation Policy Design section. If the isolated domain includes a boundary zone, then computers in the boundary zone behave just like other members of the isolated domain in the way that they interact with computers in server isolation zones.
- Isolated servers (area B) - Computers in the server isolation zones restrict access to computers, and optionally users, that authenticate as a member of a network access group (NAG) authorized to gain access.
- Encryption zone (area C) - If the data being exchanged is sufficiently sensitive, the connection security rules for the zone can also require that the network traffic be encrypted. Encryption zones are most often implemented as rules that are part of a server isolation zone, instead of as a separate zone. The diagram illustrates the concept as a subset for conceptual purposes only.

To add support for server isolation, you must ensure that the authentication methods are compatible with the requirements of the isolated server. For example, if you want to authorize user accounts that are members of a NAG in addition to authorizing computer accounts, you must enable both user and computer authentication in your connection security rules.

Important

This design builds on the Domain Isolation Policy Design, which in turn builds on the Basic Firewall Policy Design. If you plan to deploy all three designs, do the design work for all three together, and then deploy in the sequence presented.

This design can be applied to computers that are part of an Active Directory forest. Active Directory is required to provide the centralized management and deployment of Group Policy objects that contain the connection security rules.

For more information about this design:

- This design coincides with the deployment goals to Protect Computers from Unwanted Network Traffic, Restrict Access to Only Trusted Computers, Restrict Access to Only Specified Users or Computers, and Require Encryption When Accessing Sensitive Network Resources.
- To learn more about this design, see Server Isolation Policy Design Example.
- Before completing the design, gather the information described in Designing a Windows Firewall with Advanced Security Strategy.
- To help you make the decisions required in this design, see Planning Server Isolation Zones and Planning Group Policy Deployment for Your Isolation Zones.
- For a list of tasks that you can use to deploy your server isolation policy design, see "Checklist: Implementing a Server Isolation Policy Design" in the Windows Firewall with Advanced Security Deployment Guide at http://go.microsoft.com/fwlink/?linkid=98308.

Next: Certificate-based Isolation Policy Design

Certificate-based Isolation Policy Design

In the certificate-based isolation policy design, you provide the same types of protections to your network traffic as described in the Domain Isolation Policy Design and Server Isolation Policy Design sections. The only difference is the method used to authenticate your network traffic.

Domain isolation and server isolation help provide security for the computers on the network that run Windows and that can be joined to an Active Directory domain. However, in most corporate environments there are typically some computers that must run another operating system, such as Linux or UNIX. These computers cannot join an Active Directory domain. Also, some computers that do run Windows cannot join a domain for a variety of reasons. Computers that are not joined to an Active Directory domain cannot use the default Kerberos V5 protocol to authenticate.

To authenticate with non-domain member computers, IPsec supports using standards-based cryptographic certificates. Because this authentication method is also supported by many third-party operating systems, it can be used as a way to extend your isolated domain to computers that do not run Windows.

The same principles of the domain and server isolation designs apply to this design. Only computers that can authenticate (in this case, by providing a specified certificate) can communicate with the computers in your isolated domain.

For computers that run Windows and that are part of an Active Directory domain, you can use Group Policy to deploy the certificates required to communicate with the computers that are trusted but are not part of the Active Directory domain. For other computers, you will have to either manually configure them with the required certificates, or use a third-party program to distribute the certificates in a secure manner.

For more information about this design:

- This design coincides with the deployment goals to Protect Computers from Unwanted Network Traffic, Restrict Access to Only Trusted Computers, and optionally Require Encryption When Accessing Sensitive Network Resources.
- To learn more about this design, see Certificate-based Isolation Policy Design Example.
- Before completing the design, gather the information described in Designing a Windows Firewall with Advanced Security Strategy.
- To help you make the decisions required in this design, see Planning Certificate-based Authentication.
- For a list of tasks that you can use to deploy your certificate-based policy design, see "Checklist: Implementing a Certificate-based Isolation Policy Design" in the Windows Firewall with Advanced Security Deployment Guide at http://go.microsoft.com/fwlink/?linkid=98308.

Next: Evaluating Windows Firewall with Advanced Security Design Examples

Evaluating Windows Firewall with Advanced Security Design Examples

The following Windows Firewall with Advanced Security design examples illustrate how you can use Windows Firewall with Advanced Security to improve the security of the computers connected to the network. You can use these topics to evaluate how the firewall and connection security rules work across all Windows Firewall with Advanced Security designs and to determine which design or combination of designs best suits the goals of your organization.

- Firewall Policy Design Example
- Domain Isolation Policy Design Example
- Server Isolation Policy Design Example
- Certificate-based Isolation Policy Design Example

Firewall Policy Design Example

In this example, the fictitious company Woodgrove Bank is a financial services institution.

Woodgrove Bank has an Active Directory domain that provides Group Policy-based management for all their Windows-based computers. The Active Directory domain controllers also host Domain Name System (DNS) for host name resolution. Separate computers host Windows Internet Name Service (WINS) for network basic input/output system (NetBIOS) name resolution. A set of computers that are running UNIX provide the Dynamic Host Configuration Protocol (DHCP) services for automatic IP addressing.

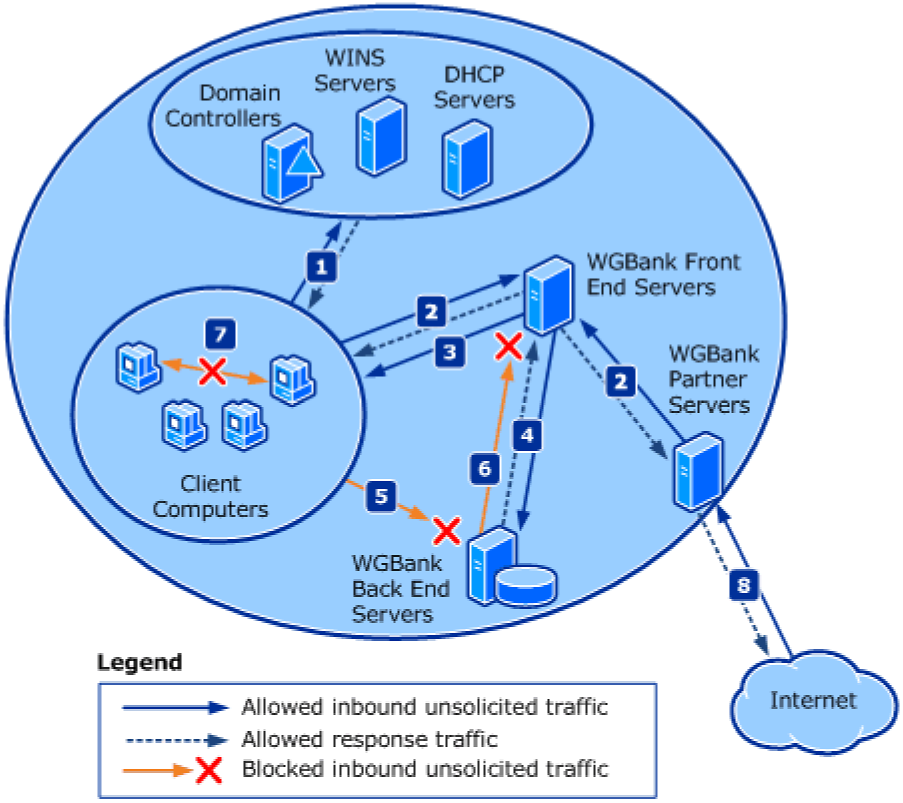
Woodgrove Bank is in the process of migrating their computers from Windows XP with Service Pack 2 (SP2) and Windows Server 2003 with SP1 to Windows Vista and Windows Server 2008. A significant number of the computers at Woodgrove Bank continue to run Windows XP with SP2 and Windows Server 2003 with SP1. Interoperability between the previous and newer operating systems must be maintained. Wherever possible, security features applied to the newer operating systems must also be applied to the previous operating systems.

A key line-of-business program called WGBank consists of a client program running on most of the desktop computers in the organization. This program accesses several front-end server computers that run the server-side part of WGBank. These front-end servers only do the processing — they do not store the data. The data is stored in several back-end database computers that are running Microsoft SQL Server.

Design requirements

The network administrators want to implement Windows Firewall with Advanced Security throughout their organization to provide an additional security layer to their overall security strategy. They want to create firewall rules that allow their business programs to operate, while blocking network traffic that is not wanted.

The following illustration shows the traffic protection needs for this design example.



1. The network infrastructure servers that are running services, such as Active Directory, DNS, DHCP, or WINS, can receive unsolicited inbound requests from network clients. The network clients can receive the responses from the infrastructure servers.

2. The WGBank front-end servers can receive unsolicited inbound traffic from the client computers and the WGBank partner servers. The WGBank client computers and partner servers can receive the response.

3. The WGBank front-end servers can send updated information to the client computers to support real-time display. The clients do not poll for this unsolicited traffic, but must be able to receive it.

4. The WGBank back-end servers can receive SQL query requests from the WGBank front-end servers. The WGBank front-end servers can receive the corresponding responses.

5. There is no direct communications between the client computers and the WGBank back-end computers.

6. There is no unsolicited traffic from the WGBank back-end computers to the WGBank front-end servers.

7. Company policy prohibits the use of peer-to-peer file transfer software. A recent review by the IT staff found that although the perimeter firewall does prevent most of the programs in this category from working, two programs are being used by staff members that do not require an outside server. Firewall rules must block the network traffic created by these programs.

8. The WGBank partner servers can receive inbound requests from partner computers through the Internet.

Other traffic notes:

- Computers are not to receive any unsolicited traffic from any computer other than specifically allowed above.
- Other outbound network traffic from the client computers not specifically identified in this example is permitted.

Design details

Woodgrove Bank uses Active Directory groups and Group Policy objects to deploy the firewall settings and rules to the computers on their network. They know that they must deploy policies to the following collections of computers:

- Client computers that run Windows XP
- Client computers that run Windows Vista
- WGBank front-end servers that run Windows Server 2003
- WGBank front-end servers that run Windows Server 2008 (there are none in place yet, but their solution must support adding them)
- WGBank partner servers that run Windows Server 2008
- WGBank back-end SQL Server computers that run Windows Server 2003
- WGBank back-end SQL Server computers that run Windows Server 2008 (there are none in place yet, but their solution must support adding them)
- Infrastructure servers that run Windows Server 2008
- Active Directory domain controllers that run Windows Server 2008
- DHCP servers that run the UNIX operating system

After evaluating these sets of computers, and comparing them to the Active Directory organizational unit (OU) structure, Woodgrove Bank network administrators determined that there was not a good one-to-one match between the OUs and the sets. Therefore the firewall GPOs will not be linked directly to OUs that hold the relevant computers. Instead, the GPOs are linked to the domain container in Active Directory, and then WMI and group filters are attached to the GPO to ensure that it is applied to the correct computers.

Setting up groups as described here ensures that you do not have to know what operating system a computer is running before assigning it to a group. A combination of WMI filters and security group filters are used to ensure that members of the group receive the GPO appropriate for the version of Windows running on that computer. For some groups, you might have four or even five GPOs.

The following groups were created by using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in, and all computers that run Windows were added to the correct groups:

- **CG_FIREWALL_ALLCOMPUTERS**. Add the predefined and system managed **Domain computers** group as a member of this group. All members of the FIREWALL_ALLCOMPUTERS group receive an operating system-specific GPO with the common firewall rules applied to all computers.

  The two computer types (client and server) are distinguished by using a WMI filters to ensure that only the policy intended for computers that are running a client version of Windows can be applied to that computer. A similar WMI filter on the server GPO ensures that only computers that are running server versions of Windows can apply that GPO. Each of the GPOs also have security group filters to prevent members of the group FIREWALL_NO_DEFAULT from receiving either of these two GPOs.

  - Client computers receive a GPO that configures Windows Firewall with Advanced Security to enforce the default Windows Firewall behavior (allow outbound, block unsolicited inbound). The client default GPO also includes the built-in firewall rule groups Core Networking and File and Printer Sharing. The Core Networking group is enabled for all profiles, whereas the File and Printer Sharing group is enabled for only the Domain and Private profiles. The GPO also includes inbound firewall rules to allow the WGBank front-end server dashboard update traffic, and rules to prevent company-prohibited programs from sending or receiving network traffic, both inbound and outbound.

  - Server computers receive a GPO that includes similar firewall configuration to the client computer GPO. The primary difference is that the rules are enabled for all profiles (not just domain and private). Also, the rules for WGBank dashboard update are not included, because it is not needed on server computers.

  All rules are scoped to allow network traffic only from computers on Woodgrove Bank's corporate network.

- **CG_FIREWALL_NO_DEFAULT**. Members of this group do not receive the default firewall GPO. Computers are added to this group if there is a business requirement for it to be exempted from the default firewall behavior. The use of a group to represent the exceptions instead of the group members directly makes it easier to support the dynamic nature of the client computer population. A new computer joined to the domain is automatically given the appropriate default firewall GPO, unless it is a member of this group.

- **CG_FIREWALL_WGB_FE**. This group contains the computer accounts for all the WGBank front-end server computers. Members of this group receive a GPO that configures Windows Firewall with Advanced Security with inbound firewall rules to allow unsolicited WGBank client traffic. Computers in this group also receive the default firewall GPO.
- **CG_FIREWALL_WGB_SQL**. This group contains the computer accounts for all the WGBank back-end computers that run SQL Server. Members of this group receive a GPO that configures Windows Firewall with Advanced Security with inbound firewall rules to allow the SQL Server program to receive unsolicited queries only from the WGBank front-end servers. Computers in this group also receive the default firewall GPO.
- **CG_FIREWALL_BOUNDARY_WGBANKFE**. This group contains the computer accounts for the servers that host Web services that can be accessed from the Internet. Members of this group receive a GPO that adds an inbound firewall rule to allow inbound HTTP and HTTPS network traffic from any address, including the Internet. Computers in this group also receive the default firewall GPO.
- **CG_FIREWALL_WINS**. This group contains the computer accounts for all the WINS server computers. Members of this group receive a GPO that configures Windows Firewall with Advanced Security with an inbound firewall rule to allow unsolicited inbound requests from WINS clients. Computers in this group also receive the default firewall GPO.
- **CG_FIREWALL_ADDC**. This group contains all the computer accounts for the Active Directory domain controller server computers. Members of this group receive a GPO that configures Windows Firewall with Advanced Security with inbound firewall rules to allow unsolicited Active Directory client and server-to-server traffic. Computers in this group also receive the default firewall GPO.

In your own design, create a group for each computer role in your organization perform that requires different or additional firewall rules. For example, file servers and print servers require additional rules to allow the incoming network traffic for those functions. If a function is ordinarily performed on most computers on the network, you might consider adding computers performing those roles to the common default firewall GPO set, unless there is a security reason not to include it there.

Next: Domain Isolation Policy Design Example

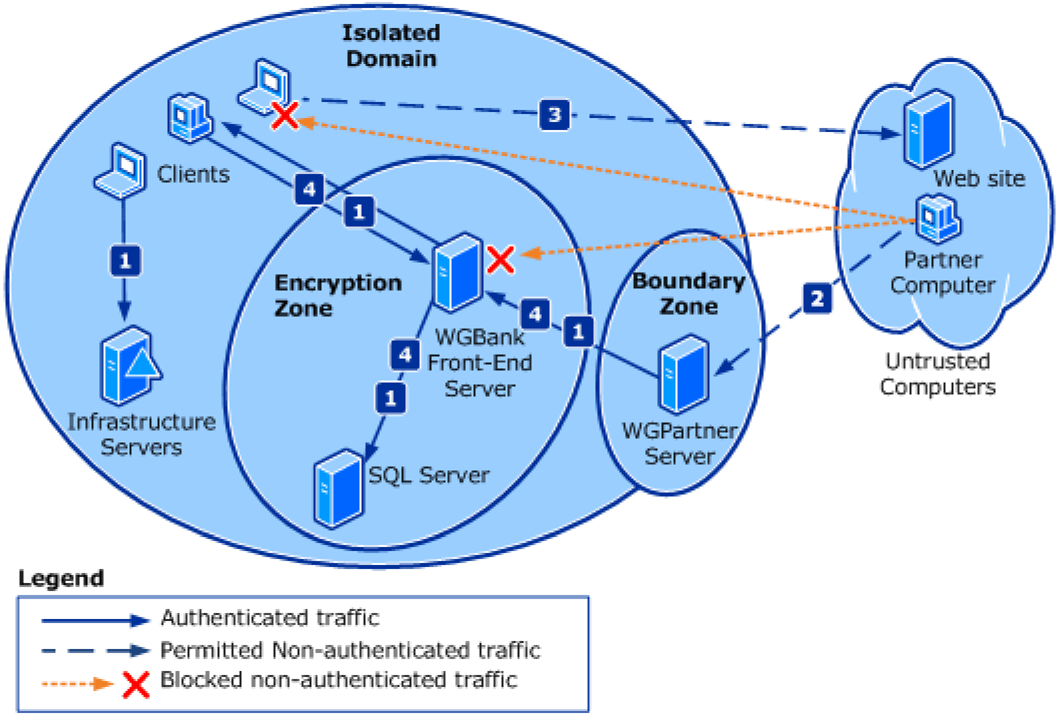
Domain Isolation Policy Design Example

This design example continues to use the fictitious company Woodgrove Bank, and builds on the example described in the Firewall Policy Design Example section. See that example for an explanation of the basic corporate network infrastructure at Woodgrove Bank with diagrams.

Design Requirements

In addition to the basic protection provided by the firewall rules in the previous design example, the administrators of the network want to implement domain isolation to provide another layer of security to their networked computers. They want to create firewall and connection security rules that use authentication to reduce the risk of communicating with untrusted and potentially hostile computers.

The following illustration shows the traffic protection needed for this design example.



1. All computers on the Woodgrove Bank corporate network that are Active Directory domain members must authenticate inbound network traffic as coming from another computer that is a member of the domain. Unless otherwise specified in this section, Woodgrove Bank's computers reject all unsolicited inbound network traffic that is not authenticated. If the basic firewall design is also implemented, even authenticated inbound network traffic is dropped unless it matches an inbound firewall rule.
2. The servers hosting the WGPartner programs must be able to receive unsolicited inbound traffic from computers owned by its partners, which are not members of Woodgrove Bank's domain.
3. Client computers can initiate non-authenticated outbound communications with computers that are not members of the domain, such as browsing external Web sites. Unsolicited inbound traffic from non-domain members is blocked.
4. Computers in the encryption zone require that all network traffic inbound and outbound must be encrypted, in addition to the authentication already required by the isolated domain.

Other traffic notes:

- All of the design requirements described in the Firewall Policy Design Example section are still enforced.

Design Details

Woodgrove Bank uses Active Directory groups and GPOs to deploy the domain isolation settings and rules to the computers on its network.

Setting up groups as described here ensures that you don't have to know what operating system a computer is running before assigning it to a group. As in the firewall policy design, a combination of WMI filters and security group filters are used to ensure that members of the group receive the GPO appropriate for the version of Windows running on that computer. For some groups, you might have four or even five GPOs.

The following groups were created by using the Active Directory Users and Computers MMC snap-in, all computers that run Windows were added to the correct groups, and then the appropriate GPO are applied to the group. To include a computer in the isolated domain or any one of its subordinate zones, simply add the computer's account in the appropriate group.

- **CG_DOMISO_ISOLATEDDOMAIN**. The members of this group participate in the isolated domain. After an initial pilot period, followed by a slowly increasing group membership, the membership of this group was eventually replaced with the entry **Domain Computers** to ensure that all computers in the domain participate by default. The WMI filters ensure that the GPO does not apply to domain controllers. GPOs with connection security rules to enforce domain isolation behavior are linked to the domain container and applied to the computers in this group. Filters ensure that each computer receives the correct GPO for its operating system type. The rules in the domain isolation GPO require Kerberos v5 authentication for inbound network connections, and request (but not require) it for all outbound connections.
- **CG_DOMISO_NO_IPSEC**. This group is denied read or apply permissions on any of the domain isolation GPOs. Any computer that cannot participate in domain isolation, such as a DHCP server running UNIX, is added to this group.
- **CG_DOMISO_BOUNDARY**. This group contains the computer accounts for all the computers that are part of the boundary group able to receive unsolicited inbound traffic from untrusted computers. Members of the group receive a GPO that configures connection security rules to request (but not require) both inbound and outbound authentication.
- **CG_DOMISO_ENCRYPTION**. This group contains the computer accounts for all the computers that require all inbound and outbound traffic to be both authenticated and encrypted. Members of the group receive a GPO that configures connection security and firewall rules to require both authentication and encryption on all inbound and outbound traffic.

Note

If you are designing GPOs for only Windows Vista and Windows Server 2008, you can design your GPOs in nested groups. For example, you can make the boundary group a member of the isolated domain group, so that it receives the firewall and basic isolated domain settings through that nested membership, with only the changes supplied by the boundary zone GPO. However, computers that are running older versions of Windows can only support a single IPsec policy being active at a time. The policies for each GPO must be complete (and to a great extent redundant with each other), because you cannot layer them as you can in the newer versions of Windows. For simplicity, this guide describes the techniques used to create the independent, non-layered policies. We recommend that you create and periodically run a script that compares the memberships of the groups that must be mutually exclusive and reports any computers that are incorrectly assigned to more than one group.

None of the groups specify which operating system is running on the computers. Because Windows XP and Windows Server 2003 use different services and have different capabilities than Windows Vista and Windows Server 2008, they must use different GPOs. Multiple GPOs must be created for each group, each with settings and rules appropriate for a specific version of Windows. A combination of WMI and security group filtering is used to ensure that members of the group receive the GPO appropriate for the version of Windows running on that computer. For more information, see Planning GPO Deployment later in this guide.

Next: Server Isolation Policy Design Example

Server Isolation Policy Design Example

This design example continues to use the fictitious company Woodgrove Bank, as described in the Firewall Policy Design Example section and the Domain Isolation Policy Design Example section.

In addition to the protections provided by the firewall and domain isolation, Woodgrove Bank wants to provide additional protection to the computers that are running Microsoft SQL Server for the WGBank program. They contain personal data, including each customer's financial history. Government and industry rules and regulations specify that access to this information must be restricted to only those users who have a legitimate business need. This includes a requirement to prevent interception of and access to the information when it is in transit over the network.

The information presented by the WGBank front-end servers to the client computers, and the information presented by the WGPartner servers to the remote partner computers, are not considered sensitive for the purposes of the government regulations, because they are processed to remove sensitive elements before transmitting the data to the client computers.

In this guide, the examples show server isolation layered on top of a domain isolation design. If you have an isolated domain, the client computers are already equipped with GPOs that require authentication. You only have to add settings to the isolated server(s) to require authentication on inbound connections, and to check for membership in the NAG. The connection attempt succeeds only if NAG membership is confirmed.

Server isolation without domain isolation

Server isolation can also be deployed by itself, to only the computers that must participate. The GPO on the server is no different from the one discussed in the previous paragraph for a server in an existing isolated domain. The difference is that you must also deploy a GPO with supporting connection security rules to the clients that must be able to communicate with the isolated server. Because those computers must be members of the NAG, that group can also be used in a security group filter on the client GPO. That GPO must contain rules that support the authentication requirements of the isolated server.

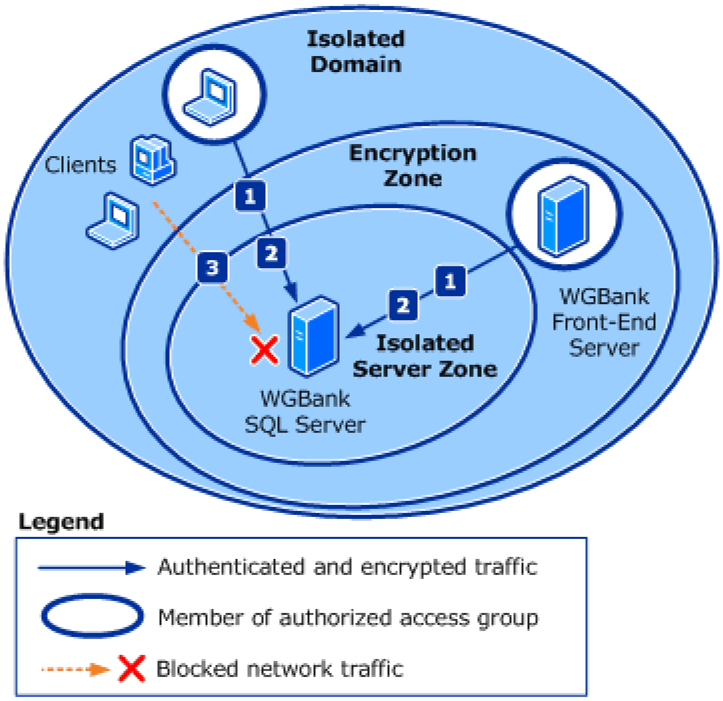
In short, instead of applying the client GPO to all clients in the domain, you apply the GPO to only the members of the NAG.

If you do not have an Active Directory domain then you can manually apply the connection security rules to the client computers, or you can use a netsh command-line script to help automate the configuration of the rules on larger numbers of computers. If you do not have an Active Directory domain, you cannot use the Kerberos V5 protocol, but instead must provide the clients and the isolated servers with certificates that are referenced in the connection security rules.

Design requirements

In addition to the protection provided by the firewall rules and domain isolation described in the previous design examples, the network administrators want to implement server isolation to help protect the sensitive data stored on the computers that run SQL Server.

The following illustration shows the traffic protection needs for this design example.



1. Access to the SQL Server computers must be restricted to only those computer or user accounts that have a business requirement to access the data. This includes the service accounts that are used by the WGBank front-end servers, and administrators of the SQL Server computers. In addition, access is only granted when it is sent from an

authorized computer. Authorization is determined by membership in a network access group (NAG).

2. All network traffic to and from the SQL Server computers must be encrypted.

3. Client computers or users whose accounts are not members of the NAG cannot access the isolated servers.

Other traffic notes:

- All of the design requirements shown in the Firewall Policy Design Example section are still enforced.

- All of the design requirements shown in the Domain Isolation Policy Design Example section are still enforced.

Design details

Woodgrove Bank uses Active Directory groups and GPOs to deploy the server isolation settings and rules to the computers on its network.

As in the previously described policy design examples, GPOs to implement the domain isolation environment are linked to the domain container in Active Directory, and then WMI filters and security group filters are attached to GPOs to ensure that the correct GPO is applied to each computer. The following groups were created by using the Active Directory Users and Computers snap-in, and all computers that run Windows were added to the correct groups.

- **CG_SRVISO_WGBANK_SQL**. This group contains the computer accounts for the computers that run SQL Server. Members of this group receive a GPO with firewall and connections security rules that require that only users who are members of the group CG_NAG_SQL_USERS can access the server, and only when they are using a computer that is a member of the group CG_NAG_SQL_COMPUTERS.

The group does not specify which operating system is running on the computer. Because Windows XP and Windows Server 2003 use different services and have different capabilities than Windows Vista and Windows Server 2008, they must use different GPOs. Multiple GPOs must be created, each one with settings and rules appropriate for a specific version of Windows. A combination of WMI and security group filtering is used to ensure that members of the group receive the GPO appropriate for the version of Windows running on that computer.

Note

If you are designing GPOs for only Windows Vista and Windows Server 2008, you can design your GPOs in nested groups. For example, you can make the isolated server group a member of the isolated domain group, so that it receives the firewall and basic isolated domain settings through that nested membership, with only the changes supplied by the isolated server GPO. However, computers that are running older versions of Windows can only support a single IPsec policy being active at a time. The policies for each GPO must be complete (and to a great extent redundant with each other), because you cannot layer them as you can in the newer versions of Windows. For simplicity, this guide describes the techniques used to create the independent, non-layered policies. We recommend that you create and periodically run a script that compares the memberships of the groups that must be mutually exclusive and reports any computers that are incorrectly assigned to more than one group.

Network access groups (NAGs) are not used to determine which GPOs are applied to a computer. Instead, these groups determine which users and computers can access the services on the isolated server.

- **CG_NAG_SQL_COMPUTERS**. This network access group contains the computer accounts that are able to access the computers running SQL Server hosting the WGBank data. Members of this group include the WGBank front-end servers, and some client computers from which SQL Server administrators are permitted to work on the servers.
- **CG_NAG_SQL_USERS**. This network access group contains the user accounts of users who are permitted to access the SQL Server computers that host the WGBank data. Members of this group include the service account that the WGBank front-end program uses to run on its computers, and the user accounts for the SQL Server administration team members.

Note

You can use a single group for both user and computer accounts. Woodgrove Bank chose to keep them separate for clarity.

If Woodgrove Bank wants to implement server isolation without domain isolation, the CG_NAG_SQL_COMPUTERS group can also be attached as a security group filter on the GPOs that apply connection security rules to the client computers. By doing this, all the computers that are authorized to access the isolated server also have the required connection security rules.

You do not have to include the encryption-capable rules on all computers. Instead, you can create GPOs that are applied only to members of the NAG, in addition to the standard domain isolation GPO, that contain connection security rules to support encryption.

Next: Certificate-based Isolation Policy Design Example

Certificate-based Isolation Policy Design Example

This design example continues to use the fictitious company Woodgrove Bank, as described in the sections Firewall Policy Design Example, Domain Isolation Policy Design Example, and Server Isolation Policy Design Example.

One of the servers that must be included in the domain isolation environment is a computer running UNIX that supplies other information to the WGBank dashboard program running on the client computers. This computer sends updated information to the WGBank front-end servers as it becomes available, so it is considered unsolicited inbound traffic to the computers that receive this information.

Design requirements

One possible solution to this is to include an authentication exemption rule in the GPO applied to the WGBank front-end servers. This rule would instruct the front-end servers to accept traffic from the non-Windows computer even though it cannot authenticate.

A more secure solution, and the one selected by Woodgrove Bank, is to include the non-Windows computer in the domain isolation design. Because it cannot join an Active Directory domain, and thus use Kerberos V5 based authentication, Woodgrove Bank chose to use certificate-based authentication. Certificates are cryptographically-protected documents, encrypted in such a way that their origin can be positively confirmed.

In this case, Woodgrove Bank used Microsoft Certificate Services, included with Windows Server 2008, to create the appropriate certificate. They might also have acquired and installed a certificate from a third-party commercial certification authority. They then used Group Policy to deploy the certificate to the front-end servers. The GPOs applied to the front-end servers also include updated connection security rules that permit certificate-based authentication in addition to Kerberos V5 authentication. They then manually installed the certificate on the UNIX server.

The UNIX server is configured with firewall and IPsec connection security rules using the tools that are provided by the operating system vendor. Those rules specify that authentication is performed by using the certificate.

The creation of the IPsec connection security rules for a non-Windows computer is beyond the scope of this document, but support for a certificate that can be used to authenticate such a non-Windows computer by using the standard IPsec protocols is the subject of this design.

The non-Windows computer can be effectively made a member of the boundary zone or the encryption zone based on the IPsec rules applied to the computer. The only constraint is that the main mode and quick mode encryption algorithms supported by the UNIX computer must also be supported by the Windows-based computers with which it communicates.

Other traffic notes:

- None of the capabilities of the other designs discussed in this guide are compromised by the use of certificate authentication by a non-Windows computer.

Design details

Woodgrove Bank uses Active Directory groups and GPOs to deploy the domain isolation settings and rules to the computers in their organization.

The inclusion of one or more non-Windows computers to the network requires only a simple addition to the GPOs for computers that must communicate with the non-Windows computer. The addition is allowing certificate-based authentication in addition to the Active Directory–supported Kerberos V5 authentication. This does not require including new rules, just adding certificate-based authentication as an option to the existing rules.

When multiple authentication methods are available, two negotiating computers agree on the first one in their lists that match. Because the majority of the computers in Woodgrove Bank's network run Windows, Kerberos V5 is listed as the first authentication method in the rules. Certificate-based authentication is added as an alternate authentication type.

By using the Active Directory Users and Computers snap-in, Woodgrove Bank created a group named NAG_COMPUTER_WGBUNIX. They then added the computer accounts to this group for Windows computers that need to communicate with the non-Windows computers. If all the computers in the isolated domain need to be able to access the non-Windows computers, then the **Domain Computers** group can be added to the group as a member.

Woodgrove Bank then created a GPO that contains the certificate, and then attached security group filters to the GPO that allow read and apply permissions to only members of the NAG_COMPUTER_WGBUNIX group. The GPO places the certificate in the **Local Computer / Personal / Certificates** certificate store. The certificate used must chain back to a certificate that is in the **Trusted Root Certification Authorities** store on the local computer.

Next: Designing a Windows Firewall with Advanced Security Strategy

Designing a Windows Firewall with Advanced Security Strategy

To select the most effective design for helping to protect the network, you must spend time collecting key information about your current computer environment. You must have a good understanding of what tasks the computers on the network perform, and how they use the network to accomplish those tasks. You must understand the network traffic generated by the programs running on the computers.

- Gathering the Information You Need
- Determining the Trusted State of Your Computers

The information that you gather will help you answer the following questions. The answers will help you understand your security requirements and select the design that best matches those requirements. The information will also help you when it comes time to deploy your design, by helping you to build a deployment strategy that is cost effective and resource efficient. It will help you project and justify the expected costs associated with implementing the design.

- What traffic must always be allowed? What are characteristics of the network traffic generated and consumed by the business programs?
- What traffic must always be blocked? Does your organization have policies that prohibit the use of specific programs? If so, what are the characteristics of the network traffic generated and consumed by the prohibited programs?
- What traffic on the network cannot be protected by IPsec because the computers or devices sending or receiving the traffic do not support IPsec?
- For each type of network traffic, does the default configuration of the firewall (block all unsolicited inbound network traffic, allow all outbound traffic) allow or block the traffic as required?
- Do you have an Active Directory domain (or forest of trusted domains) to which all your computers are joined? If you do not, then you cannot use Group Policy for easy mass deployment of your firewall and connection security rules. You also cannot easily take advantage of Kerberos V5 authentication that all domain clients can use.
- Which computers must be able to accept unsolicited inbound connections from computers that are not part of the domain?
- Which computers contain data that must be encrypted when exchanged with another computer?

- Which computers contain sensitive data to which access must be restricted to specifically authorized users and computers?
- Does your organization have specific network troubleshooting devices or computers (such as protocol analyzers) that must be granted unlimited access to the computers on the network, essentially bypassing the firewall?

If you already have firewall or IPsec rules deployed

Windows Firewall with Advanced Security in Windows Vista and Windows Server 2008 has many new capabilities that are not available in earlier versions of Windows. The IPsec and Windows Firewall policies that you create for computers that are running Windows XP and Windows Server 2003 can still be applied to computers that are running Windows Vista and Windows Server 2008. However, doing this prevents you from taking advantage of all the new features performance improvements included in Windows Vista and Windows Server 2008.

If you already have a domain and/or server isolation deployment in your organization then you must evaluate and choose between two options:

- **Option 1:** Use the existing GPOs already in place and apply them to computers that are running Windows Vista and Windows Server 2008. If you choose to do this then you must use the Windows Firewall and IPsec guidance applicable to Windows XP and Windows Server 2003. Design and deployment guidance for those technologies is available on the Web at "Server and Domain Isolation Using IPsec and Group Policy" (http://go.microsoft.com/fwlink/?linkid=110400). It is also available in downloadable form at http://go.microsoft.com/fwlink/?linkid=110401.
- **Option 2:** Create new GPOs for computers that are running Windows Vista and Windows Server 2008, and use WMI and group filters to ensure that the correct GPOs apply to your computers. This is the technique discussed in this guide and its accompanying deployment guide.

If you choose this technique, you must ensure that the IPsec policies you apply to your computers that are running different operating systems are compatible with each other. For example, a server that is running Windows Server 2008 can use a broader set of authentication and encryption settings than are available on Windows XP and Windows Server 2003. To ensure that client computers that are running both older and newer operating systems can access the resources on a server, the server must include in its IKE negotiation offers at least one algorithm that each client can use. You can choose to use the newer, more advanced settings to help secure traffic to a client that is running Windows Vista, but if the server must also be accessed by computers that are running previous versions of Windows, then the server must also offer authentication methods that those computers can use.

This guide describes how to plan your groups and GPOs for an environment with a mix of operating systems. Details can be found in the section Planning Group Policy Deployment for Your Isolation Zones later in this guide.

Next: Gathering the Information You Need

Gathering the Information You Need

Before starting the planning process for a Windows Firewall with Advanced Security deployment, you must collect and analyze up-to-date information about the network, the directory services, and the computers that are already deployed in the organization. This information enables you to create a design that accounts for all possible elements of the existing infrastructure. If the gathered information is not accurate, problems can occur when devices and computers that were not considered during the planning phase are encountered during implementation.

Review each of the following topics for guidance about the kinds of information that you must gather:

- Gathering Information about Your Current Network Infrastructure
- Gathering Information about Your Active Directory Deployment
- Gathering Information about Your Computers
- Gathering Other Relevant Information

Gathering Information about Your Current Network Infrastructure

Perhaps the most important aspect of planning for Windows Firewall with Advanced Security deployment is the network architecture, because IPsec is layered on the Internet Protocol itself. An incomplete or inaccurate understanding of the network can prevent any Windows Firewall with Advanced Security solution from being successful. Understanding subnet layout, IP addressing schemes, and traffic patterns are part of this effort, but accurately documenting the following components are important to completing the planning phase of this project:

- **Network segmentation**. This includes IP addressing maps, showing how your routers separate each network segment. It includes information about how the routers are configured, and what security filters they impose on network traffic flowing through them.
- Network address translation (NAT). NAT is a means of separating network segments by using a device that maps all of the IP addresses on one side of the device to a single IP address accessible on the other side.
- Network infrastructure devices. This includes the routers, switches, hubs, and other network equipment that makes communications between the computers on the network possible.
- **Current network traffic model.** This includes the quantity and the characteristics of the network traffic flowing through your network.

The goal is to have enough information to be able to identify an asset by its network location, in addition to its physical location.

Do not use a complex and poorly documented network as a starting point for the design, because it can leave too many unidentified areas that are likely to cause problems during implementation.

This guidance helps obtain the most relevant information for planning Windows Firewall with Advanced Security implementation, but it does not try to address other issues, such as TCP/IP addressing or virtual local area network (VLAN) segmentation.

Network segmentation

If your organization does not have its current network architecture documented and available for reference, such documentation should be obtained as soon as possible before you continue with the design and deployment. If the documented information is not current or has not been validated recently, you have two options:

- Accept that the lack of accurate information can cause risk to the project.
- Undertake a discovery project, either through manual processes or with network analysis tools that can provide the information you need to document the current network topology.

Although the required information can be presented in many different ways, a series of schematic diagrams is often the most effective method of illustrating and understanding the current network configuration. When creating network diagrams, do not include too much information. If necessary, use multiple diagrams that show different layers of detail. Use a top-level diagram that illustrates the major sites that make up your organization's network, and then break out each site into a more detailed diagram that captures a deeper level of detail. Continue until you reach the individual IP subnet level, and so have the means to identify the network location of every computer in your organization.

During this process, you might discover some network applications and services that are not compatible with IPsec. For example, IPsec breaks network-based prioritization and port/protocol-based traffic management. If traffic management or prioritization must be based on ports or protocol, the host itself must be able to perform any traffic management or prioritization.

Other examples of incompatibility include:

- Cisco NetFlow on routers cannot analyze packets between IPsec members based on protocol or port.
- Router-based Quality of Service (QoS) cannot use ports or protocols to prioritize traffic. However, using firewall rules that specify IP addresses to prioritize traffic are not affected by this limitation of QoS. For example, a rule that says "From anyone to anyone using port 80 prioritize" does not work, but a rule that says "From anyone to 10.0.1.10 prioritize" works.
- Weighted Fair Queuing and other flow-based router traffic priority methods might fail.
- Devices that do not support or allow IP protocol 50, the port that is used by Encapsulating Security Payload (ESP).
- Router access control lists (ACLs) cannot examine protocol and port fields in ESP-encrypted packets, and therefore the packets are dropped. ACLs based only on IP address are forwarded as usual. If the device cannot parse ESP, any ACLs that specify port or protocol rules will not be processed on the ESP packets. If the device has an ESP parser and uses encryption, ACLs that specify port or protocol rules will not be processed on the ESP packets.
- Network monitoring tools might be unable to parse ESP packets that are not encrypted (ESP-Null).

Note

Network Monitor added an ESP parser starting in version 2.1 to aid troubleshooting of unencrypted IPsec packets. The latest version of Network Monitor is available as a free download from Microsoft (http://go.microsoft.com/fwlink/?linkid=94770).

Network address translation (NAT)

Special consideration is required if NAT devices are present and separate some of the network segments from others. NAT blocks the use of Authentication Header (AH) between computers that are separated by a NAT device. If NAT devices exist on the internal network then you must specify ESP instead of AH. ESP allows you to encrypt data, but does not require encryption. ESP can be implemented by using null encryption, which provides the strongest IPsec peer-to-peer communication possible without breaking communications through NAT.

IPsec NAT traversal (NAT-T) enables IPsec peers that are behind NATs to detect the presence of NATs, negotiate IPsec security associations (SAs), and send ESP-protected data even though the addresses in the IPsec-protected IPv4 packets change. IPsec NAT-T does not support the use of AH across NAT devices.

IPsec NAT-T is supported by Windows Vista, Windows Server 2008, Windows Server 2003 with SP1, Windows XP with SP2, and by Windows 2000 Server with SP4 with a free Web download. For more information, see "L2TP/IPsec NAT-T update for Windows XP SP1 and Windows 2000 Server at http://go.microsoft.com/fwlink/?LinkId=45084. This is a client-side update only, and does not enable a computer that is running Windows 2000 Server to receive an incoming IPsec protected connection from a client computer that is behind a NAT device.

For detailed information about how IPsec NAT-T works, see "IPsec NAT Traversal Overview" in the August 2002 Cable Guy article at http://go.microsoft.com/fwlink/?LinkId=45080.

Do not put servers behind NAT devices

Do not put servers that must be available to public IPsec clients on the private networks behind NAT devices. Windows XP with SP2 and later operating systems by default do not support establishing IPsec connection to servers that are located on the private network behind a NAT device. For more information, see "IPsec NAT-T is Not Recommended for Windows Server Computers that are Behind Network Address Translators" at http://go.microsoft.com/fwlink/?LinkId=45083.

This only affects servers behind the NAT device. The article does not apply to client computers.

For more information about the challenges and risks associated with positioning servers behind NAT devices, see "Problems with Using Network Address Translators" in the October 2004 Cable Guy article at http://go.microsoft.com/fwlink/?LinkId=45081.

If you must locate a server on the private network behind a NAT device, then you must do the following:

- Configure the Windows clients that must access the server to enable IPsec security associations to servers that are located behind a NAT device. For instructions about how to configure the clients for that scenario, see "L2TP/IPsec NAT-T update for Windows XP SP1 and Windows 2000 Server at http://go.microsoft.com/fwlink/?LinkId=45084. The instructions apply to all later service packs of Windows XP, although the download itself is only applicable to SP1. This can be especially challenging if the client computers that need access to the server are not managed by your organization.

- To ensure that a server is reachable from behind a NAT device for IPsec traffic, you must configure the NAT device with static translation entries that map IKE (using UDP port 500) and IPsec NAT-T (using UDP port 4500) traffic to the correct server.

Network infrastructure devices

The devices that make up the network infrastructure (routers, switches, load balancers, and firewalls) must be able communicate using IPsec after the solution is implemented. For this reason, you have to examine the following characteristics of these network devices to ensure that they can handle the technical and physical requirements of the design:

- **Make/model**. You can use this information to determine the features that the device supports. In addition, check the BIOS version or software running on the device to ensure that IPsec is supported.
- **Amount of RAM**. This information is useful when you are analyzing capacity or the impact of IPsec on the device.
- **Traffic analysis**. Information, such as peak usage and daily orweekly trends, is helpful to have. The information helps provide a baseline snapshot of the device and how it is used over time. If problems occur after IPsec is implemented, the information can help determine whether the root cause is related to greater usage of the device.
- **Router ACLs that affect IPsec directly**. ACLs directly affect the ability of specific protocols to function. For example, blocking the Kerberos V5 protocol (UDP and TCP port 88) or IP protocol 50 or 51 prevents IPsec from working. Devices must also be configured to allow IKE traffic (UDP port 500) if using NAT-T (UDP port 4500).
- **Networks/subnets connected to device interfaces**. This information provides the best picture of what the internal network looks like. Defining the boundary of subnets based on an address range is straightforward and helps identify whether other addresses are either unmanaged or foreign to the internal network (such as IP addresses on the Internet).
- **VLAN segmentation**. Determining how VLANs are implemented on the network can help you understand traffic patterns and security requirements, and then help to determine how IPsec might augment or interfere with these requirements.
- **The maximum transmission unit (MTU) size on device interface(s)**. The MTU defines the largest datagram that can be transmitted on a particular interface without being divided into smaller pieces for transmission (a process also known as *fragmentation*). In IPsec communications, the MTU is necessary to anticipate when fragmentation occurs. Packet fragmentation must be tracked for Internet Security Association and Key Management Protocol (ISAKMP) by the router. IPsec configures the MTU size on the session to the minimum-discovered MTU size along the communication path being used, and then set the Don't Fragment bit (DF bit) to 1.

Note

If Path MTU (PMTU) discovery is enabled and functioning correctly, you do not have to gather the MTU size on device interfaces. Although sources, such as the Windows Server 2003 Hardening Guide, recommend disabling PMTU discovery, it must be enabled for IPsec to function correctly.

- **Intrusion detection system (IDS) in use**. Your IDS must have an IPsec-compatible parser to interpret data inside secured packets. If the IDS does not have such a parser, it cannot examine data in those packets to determine whether a particular session is a potential threat.

After you obtain this information, you can quickly determine whether you must upgrade the devices to support the requirements of the project, change the ACLs, or take other measures to ensure that the devices can handle the loads needed.

Current network traffic model

After gathering the addressing and network infrastructure information, the next step is to examine the communications flow. For example, if a department such as Human Resources (HR) spans several buildings, and you want to use server isolation with encryption to help protect information in that department, you must know how those buildings are connected to determine the level of "trust" to place in the connection. A highly secured building that is connected by an unprotected cable to another building that is not secured can be compromised by an eavesdropping or information replay attack. If such an attack is considered a threat, IPsec can help by providing strong mutual authentication and traffic encryption for trusted hosts. However, the solution cannot account for the fact that a lack of physical security on trusted hosts will remain a threat.

When you examine traffic flow, look closely at how all managed and unmanaged devices interact. This includes non-Windows-based computers running Linux, UNIX, and Macintosh. Ask yourself such questions as, Do specific communications occur at the port and protocol level, or are there many sessions between the same hosts across many protocols? How do servers and clients communicate with each other? Are there security devices or projects currently implemented or planned that could affect an isolation deployment? For example, if you use Windows Firewall on your computers to "lock down" specific ports, such as UDP 500, IKE negotiations fail.

Some of the more common applications and protocols are as follows:

- **NetBIOS over TCP/IP (NetBT) and server message block (SMB)**. On a LAN, it is common to have ports 137, 138, and 139 enabled for NetBT and port 445 enabled for SMB. These ports provide NetBIOS name resolution services and other features. Unfortunately, they also allow the creation of *null sessions*. A null session is a session that is established on a host that does not use the security context of a known user or entity. Frequently, these sessions are anonymous.
- **Remote procedure call (RPC)**. RPC operates by listening on a port known as the *endpoint mapper*, TCP port 135. The response to a query on this port is an instruction to begin communication on another port in the ephemeral range (ports numbered over 1024). In a network that is segmented by firewalls, RPC communication presents a configuration challenge because it means opening the RPC listener port and all ports greater than 1024. Opening so many ports increases the attack surface of the whole

network and reduces the effectiveness of the firewalls. Computers running Windows Vista and Windows Server 2008 reduce this risk by introducing stateful inspection of RPC traffic. Because many applications depend on RPC for basic functionality, any firewall and connection security policy must take RPC requirements into account.

- **Other traffic**. Windows Firewall with Advanced Security can help secure transmissions between computers by providing authentication of the packets in addition to encrypting the data that they contain. The important thing to do is to identify what must be protected, and the threats that must be mitigated. Examine and model other traffic or traffic types that must be secured.

Next: Gathering Information about Your Active Directory Deployment

Gathering Information about Your Active Directory Deployment

Active Directory is another important item about which you must gather information. You must understand the forest structure. This includes domain layout, organizational unit (OU) architecture, and site topology. This information makes it possible to know where computers are currently placed, their configuration, and the impact of changes to Active Directory that result from implementing Windows Firewall with Advanced Security. Review the following list for information needed:

- **Names and number of forests**. The forest (not the domain) is the security boundary in an Active Directory implementation. You must understand the current Active Directory architecture to determine the most effective strategy for deploying your firewall and connection security rules using Group Policy. It also enables you to understand which computers can be isolated and how best to accomplish the required degree of isolation.
- **Names and number of domains**. Authentication in server and domain isolation uses the IKE negotiation process with the Kerberos V5 protocol. This protocol assumes that computers are domain members.
- **Number and types of trusts**. Trusts affect the logical boundaries of domain isolation and define whether IKE negotiation can occur between computers in different Active Directory domains.
- **Names and number of sites**. Site architecture is usually aligned with the network topology. Understanding how sites are defined in Active Directory will help provide insight into replication and other details. Site architecture can provide a better understanding of the current Active Directory deployment.
- **OU structure**. OUs are logical constructs and can therefore be molded to fit many different requirements and goals. The OU structure is an ideal place to examine how Group Policy is currently used and how the OUs are laid out. You do not have to redesign an already implemented OU structure in order to effectively deploy firewall and connection security policy, but an understanding of the structure helps you know what WMI or group filtering is required to apply each GPO to the correct computers.
- **Existing IPsec policy**. Because this project culminates in the implementation of IPsec policy, you must understand how the network currently uses IPsec (if at all). Windows Firewall with Advanced Security connection security rules for Windows Vista

and Windows Server 2008 are not compatible with earlier versions of Windows. If you already have IPsec policies deployed to computers running Windows XP and Windows Server 2003 in your organization, you must ensure that the new IPsec policies you deploy enable computers using either the old or new IPsec policies to communicate with each other.

Next: Gathering Information about Your Computers

Gathering Information about Your Computers

One of the most valuable benefits of conducting an asset discovery project is the large amount of data that is obtained about the client and server computers on the network. When you start designing and planning your isolation zones, you must make decisions that require accurate information about the state of all hosts to ensure that they can use IPsec as planned.

Capture the following information from each computer:

- **Computer name**. This name is the computer's NetBIOS or DNS name that identifies the computer on the network. Because a computer can have more than one media access control (MAC) or IP address, the computer's name is one of the criteria that can be used to determine uniqueness on the network. Because computer names can be duplicated under some circumstances, the uniqueness should not be considered absolute.
- **IP address for each network adapter**. The IP address is the address that is used with the subnet mask to identify a host on the network. An IP address is not an effective way to identify an asset because it is often subject to change.
- **MAC address for each network adapter**. The MAC address is a unique 48-bit address that is used to identify a network adapter. It can be used to help differentiate between different network adapters on the same device.
- **Operating system, service pack, and hotfix versions**. The operating system version is a key factor in determining the ability of a host to communicate by using IPsec. It is also important to track the current state of service packs and updates that might be installed, because these are often used to determine that minimum security standards have been met.
- **Domain membership**. This information is used to determine whether a computer can obtain IPsec policy from Active Directory or whether it must use a local IPsec policy.
- **Physical location**. This information is just the location of the device in your organization. It can be used to determine whether a device can participate in a specific isolation group based on its location or the location of the devices that it communicates with regularly.
- **Hardware type or role**. Some tools that perform host discovery can provide this information by querying the hardware information and running applications to determine its type, such as server, workstation, or portable computer. You can use this information to determine the appropriate IPsec policy to assign, whether a specific computer can participate in isolation, and in which isolation group to include the computer.

After collecting all this information and consolidating it into a database, perform regular discovery efforts periodically to keep the information current. You need the most complete and up-to-date picture of the managed hosts on their networks to create a design that matches your organization's requirements.

You can use various methods to gather data from the hosts on the network. These methods range from high-end, fully automated systems to completely manual data collection. Generally, the use of automated methods to gather data is preferred over manual methods for reasons of speed and accuracy.

Automated Discovery

Using an automated auditing network management system such as Microsoft System Center Configuration Manager (formerly known as Systems Management Server) provides valuable information about the current state of the IT infrastructure.

For more information about how System Center Configuration Manager 2007 can help perform automated information gathering, see http://go.microsoft.com/fwlink/?linkid=110412.

Manual Discovery

The biggest difference between manual discovery methods and automated methods is time.

You can use the Windows Script Host (WSH), VBScript, and Windows Management Instrumentation (WMI) to create a script file that can collect the system configuration information. VBScript and WMI are built-in to Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. In addition, PowerShell is available as a free download for computers that run Windows XP, Windows Server 2003, or later versions. Starting with Windows Server 2008, PowerShell is included with the operating system. For more information, see http://go.microsoft.com/fwlink/?linkid=110413.

Whether you use an automatic, manual, or hybrid option to gather the information, one of the biggest issues that can cause problems to the design is capturing the changes between the original inventory scan and the point at which the implementation is ready to start. After the first scan has been completed, make support staff aware that all additional changes must be recorded and the updates noted in the inventory.

This inventory will be critical for planning and implementing your Windows Firewall with Advanced Security design.

Next: Gathering Other Relevant Information

Gathering Other Relevant Information

This topic discusses several other things that you should examine to see whether they will cause any complications in your ability to deploy Windows Firewall with Advanced Security policies in your organization.

Capacity considerations

Because IPsec uses mathematically intensive cryptographic techniques, it can consume significant overhead on a computer. Areas to watch:

- **Encryption.** You might use 256-bit Advanced Encryption Standard (AES-256) and 384-bit Secure Hash Algorithm (SHA-384) to check integrity in situations that require the strongest available encryption and key exchange protection.
- **Security association (SA) negotiation.** You can use a shorter lifetime for the main mode SA, such as three hours, but then you might need to make tradeoffs. Because each main mode SA occupies approximately 5 KB of RAM, situations in which a server brokers tens of thousands of concurrent connections can lead to overutilization.
- **NAT devices.** As discussed earlier, NAT does not allow Authentication Header (AH) conversations between hosts. If NAT devices exist on the internal network, ESP must be selected instead of AH. ESP provides for the ability to encrypt data, but does not require encryption. ESP null encryption provides the strongest IPsec peer-to-peer communication through NAT. And because it does not use encryption, it has a lower impact than ESP with encryption.
- **Switches and routers.** Proper capacity planning for the implementation of IPsec is more about thorough testing and expected traffic loads than exact calculations. You might have to upgrade or reconfigure switches or routers that currently exceed 75 percent usage to allow for increased traffic on the device and still provide some extra usage for bursts of traffic.
- **Other factors.** These include CPU usage on network infrastructure servers, increased overhead on servers and workstations running IPsec (especially servers, because they usually contain more main mode SAs than clients), and increased network latency because of IPsec negotiation.

Note

When Microsoft deployed its own domain isolation solution, it found a one to three percent increase in usage on the network as a direct result of IPsec.

Group Policy deployment groups and WMI filters

You do not have to rearrange the organization unit (OU) hierarchy of your Active Directory domains to effectively deploy Windows Firewall with Advanced Security GPOs. Instead, you can link your GPOs at the domain level (or another high level container), and then use security group filtering or WMI filtering to ensure that only the appropriate computers or users can apply the GPO settings. Because the firewall and connection security rules have evolved significantly from Windows 2000 Server to Windows XP and Windows Server 2003, and now with Windows Vista and Windows Server 2008, we recommend that you use WMI filtering to dynamically ensure that GPOs apply only to computers that are running the correct operating system. If you have computers that are running Windows 2000 Server, WMI filtering is not available, and you must create a computer group to contain the accounts for those computers, and then apply security permissions to GPOs for all later operating systems so that other members of that group do not apply the GPOs. The Woodgrove Bank examples throughout this guide illustrate the technique.

Different Active Directory trust environments

When you design a domain isolation policy, consider any logical boundaries that might affect IPsec-secured communications. For example, the trust relationships between your domains and forests are critical in determining an appropriate IKE authentication method.

Kerberos V5 authentication is recommended for use in a two-way (mutual) domain and forest trust environment. You can use Kerberos V5 for IKE authentication across domains that have two-way trusts established, if the domains are in the same forest or different forests. If the two domains are in different forests, you must configure two external trusts, one for each direction, between the domains. The external trusts must use the fully qualified domain name (FQDN) of the domains, and IPsec policy must allow an IKE initiator in one domain to communicate with any domain controller in the forest domain hierarchy, so that the initiator can obtain a Kerberos V5 ticket from a domain controller in the responder’s domain. If firewalls separate the domains then you must configure the firewall to allow Kerberos V5 traffic over UDP destination port 88, TCP destination port 88, and UDP destination port 389.

For more information, see "Active Directory in Networks Segmented by Firewalls" at http://go.microsoft.com/fwlink/?LinkId=45087.

If the use of Kerberos V5 authentication is not possible because two-way trusts across forests cannot be established as in some large enterprise environments, you can use a public key infrastructure (PKI) and digital certificates to establish IPsec-trusted communication. For an example of how Microsoft deployed their PKI, see "Deploying PKI Inside Microsoft" at http://go.microsoft.com/fwlink/?LinkId=45088.

Creating firewall rules to permit ISAKMP, AH, and ESP traffic

In some cases, IPsec-secured traffic might have to pass through a router, perimeter firewall, or other filtering device. In the case of a router, unless the router filters TCP and UDP traffic or other upper-level protocol headers, no special configuration is required to allow the IPsec traffic to be forwarded.

In the case of a filtering router or a firewall, you must configure these devices to allow IPsec traffic to be forwarded. Configure the firewall to allow IPsec traffic on UDP source and destination port 500 (ISAKMP), UDP source and destination port 4500 (IPsec NAT-T), and IP Protocol 50 (ESP). You might also have to configure the firewall to allow IPsec traffic on IP protocol 51 (AH) to allow troubleshooting by IPsec administrators and to allow the IPsec traffic to be inspected.

For more information, see "How to Enable IPsec Traffic Through a Firewall" at http://go.microsoft.com/fwlink/?LinkId=45085.

Network load balancing and server clusters

There are challenges implementing connection security for network traffic going to and from network load balancing (NLB) clusters and server clusters. NLB enables multiple servers to be clustered together to provide high availability for a service by providing automatic failover to other nodes in the cluster. Because IPsec matches a security association to a specific computer, it prevents different computers from handling the same client connection. If a different node in the cluster responds to an IPsec connection that was originally established by another node, the traffic will be dropped by the client computer as untrusted.

This means that NLB in "no affinity" mode is not supported by IPsec at all. If you must use "no affinity" mode in the cluster then consider including the servers that make up the cluster in your IPsec exemption group, and allowing clients to communicate with the servers without IPsec.

Issues with IPsec on clusters running on Windows 2000 Server or Windows Server 2003

Even when not using "no affinity" mode there are challenges. If a node in the cluster fails, existing IPsec connections to that server cannot detect the failover, but attempt to rebuild the security association until the preset time-out period expires. In Windows 2000 Server, IPsec must be idle for five minutes before the client attempts to re-authenticate. This causes a two-to-six minute interruption in service for that client. Windows XP with SP2, and Windows Server 2003 with SP1 reduce the preset time-out period to one minute. There will always be a delay if a client is connected to a cluster node that fails.

For more information about IPsec and configuring NLB clusters, see the following articles on the Microsoft Support Site:

- "How to Configure Network Load Balancing to Work with IPsec" at http://go.microsoft.com/fwlink/?LinkId=45089
- "IPsec is not designed for failover" at http://go.microsoft.com/fwlink/?LinkId=45091
- "How to Configure IPsec on an Exchange Server 2003 Back-End Server That Is Running on a Windows Server 2003 Server Cluster" at http://go.microsoft.com/fwlink/?LinkId=45092

IPsec improvements for clusters running Windows Server 2008

In Windows Server 2008, IPsec is much more tightly integrated into TCP/IP than in earlier versions of Windows. When a TCP connection is dropped because of a cluster node failover, IPsec on a computer that is running Windows Vista and Windows Server 2008 detects the TCP connection failure and removes the IPsec SAs for that connection. When the new TCP connection is established to another node, IPsec can negotiate new SAs immediately without having to wait for the obsolete SAs to time out.

Network inspection technologies

Within a TCP/IP packet, IPsec without encryption changes the offsets for the destination ports and protocols. These changes can adversely affect applications that are running on network devices such as routers that monitor and manage traffic on the network. While some network applications have been updated to support IPsec, some are not yet compatible. Check with the vendor of your device to see whether the changes in the protocol and port fields caused by IPsec are compatible with the device.

Any device designed to view network traffic, such as hardware protocol analyzers or Microsoft Network Monitor, cannot parse ESP-encrypted traffic. Only the destination computer, with which the originating computer negotiated the connection, can decrypt the traffic.

In general, IPsec defeats network-based prioritization and port- or protocol-based traffic management. For encrypted packets, there is no workaround; the host itself must handle any traffic management functions. For unencrypted, authenticated-only packets, the devices and applications must be aware of how IPsec changes packets to be able to do anything with them other than route them to the correct host. If you cannot upgrade monitoring or management devices to support IPsec, it is important that you record this information and figure it into your domain or server isolation design.

Network Monitor includes parsers for the ISAKMP (IKE), AH, and ESP protocols. Network Monitor parsers for ESP can parse inside the ESP packet only if ESP null-encryption is being used. Network Monitor cannot parse the encrypted parts of IPsec ESP traffic when encryption is performed in software. However, if encryption is performed by an IPsec hardware offload network adapter, the ESP packets can be decrypted when Network Monitor captures them on either the source or the destination and, therefore, they can be parsed. To diagnose ESP software-encrypted communication, you must disable ESP encryption and use ESP-null encryption by changing the IPsec policy or connection security rule on both computers.

Network Monitor is available as a free download from Microsoft at http://go.microsoft.com/fwlink/?linkid=94770.

Next: Determining the Trusted State of Your Computers

Determining the Trusted State of Your Computers

After obtaining information about the computers that are currently part of the IT infrastructure, you must determine at what point a computer is considered trusted. The term *trusted* can mean different things to different people. Therefore, you must communicate a firm definition for it to all stakeholders in the project. Failure to do this can lead to problems with the security of the trusted environment, because the overall security cannot exceed the level of security set by the least secure client that achieves trusted status.

Note

> In this context, the term *trust* has nothing to do with an Active Directory trust relationship between domains. The trusted state of your computers just indicates the level of risk that you believe the computer brings to the network. Trusted computers bring little risk whereas untrusted computers can potentially bring great risk.

Trust states

To understand this concept, consider the four basic states that apply to computers in a typical IT infrastructure. These states are (in order of risk, lowest risk first):

1. Trusted
2. Trustworthy
3. Known, untrusted
4. Unknown, untrusted

The remainder of this section defines these states and how to determine which computers in your organization belong in each state.

Trusted state

Classifying a computer as trusted means that the computer's security risks are managed, but it does not imply that it is perfectly secure or invulnerable. The responsibility for this managed state falls to the IT and security administrators, in addition to the users who are responsible for the configuration of the computer. A trusted computer that is poorly managed will likely become a point of weakness for the network.

When a computer is considered trusted, other trusted computers can reasonably assume that the computer will not initiate a malicious act. For example, trusted computers can expect that other trusted computers will not run a virus that attacks them, because all trusted computers are required to use mechanisms (such as antivirus software) to mitigate the threat of viruses.

Spend some time defining the goals and technology requirements that your organization considers appropriate as the minimum configuration for a computer to obtain trusted status.

A possible list of technology requirements might include the following:

- **Operating system.** A trusted client computer should run Windows Vista or Windows XP with SP2. A trusted server should run Windows Server 2008 or Windows Server 2003.
- **Domain membership.** A trusted computer will belong to a managed Active Directory domain, which means that the IT department has security management rights and can configure member computers by using Group Policy.
- **Management client.** All trusted computers must run a specific network management client to allow for centralized management and control of security policies, configurations, and software. Microsoft System Center Configuration Manager is one such management system with an appropriate client. For more information, see http://go.microsoft.com/fwlink/?linkid=110412.
- **Antivirus software.** All trusted computers will run antivirus software that is configured to check for and automatically update the latest virus signature files daily. Microsoft ForeFront Client Security is one such antivirus software program. For more information, see http://go.microsoft.com/fwlink/?linkid=110479.
- **File system.** All trusted computers will be configured to use the NTFS file system.
- **BIOS settings.** All trusted portable computers will be configured to use a BIOS-level password that is under the management of the IT support team.
- **Password requirements.** Trusted clients must use strong passwords.

It is important to understand that the trusted state is not constant; it is a transitive state that is subject to changing security standards and compliance with those standards. New threats and new defenses emerge constantly. For this reason, the organization's management systems must continually check the trusted computers to ensure ongoing compliance. Additionally, the management systems must be able to issue updates or configuration changes if they are required to help maintain the trusted status.

A computer that continues to meet all these security requirements can be considered trusted. However it is possible that most computers that were identified in the discovery process discussed earlier do not meet these requirements. Therefore, you must identify which computers can be trusted and which ones cannot. To help with this process, you use the intermediate *trustworthy* state. The remainder of this section discusses the different states and their implications.

Trustworthy state

It is useful to identify as soon as possible those computers in your current infrastructure that can achieve a trusted state. A *trustworthy state* can be assigned to indicate that the current computer can physically achieve the trusted state with required software and configuration changes.

For each computer that is assigned a trustworthy status, make an accompanying configuration note that states what is required to enable the computer to achieve trusted status. This information is especially important to both the project design team (to estimate the costs of adding the computer to the solution) and the support staff (to enable them to apply the required configuration).

Generally, trustworthy computers fall into one of the following two groups:

- **Configuration required.** The current hardware, operating system, and software enable the computer to achieve a trustworthy state. However, additional configuration changes are required. For example, if the organization requires a secure file system before a computer can be considered trusted, a computer that uses a FAT32-formatted hard disk does not meet this requirement.
- **Upgrade required.** These computers require upgrades before they can be considered trusted. The following list provides some examples of the type of upgrade these computers might require:
    - **Operating system upgrade required.** If the computer's current operating system cannot support the security needs of the organization, an upgrade would be required before the computer could achieve a trusted state.
    - **Software required.** A computer that is missing a required security application, such as an antivirus scanner or a management client, cannot be considered trusted until these applications are installed and active.
    - **Hardware upgrade required.** In some cases, a computer might require a specific hardware upgrade before it can achieve trusted status. This type of computer usually needs an operating system upgrade or additional software that forces the required hardware upgrade. For example, security software might require additional hard disk space on the computer.
    - **Computer replacement required.** This category is reserved for computers that cannot support the security requirements of the solution because their hardware cannot support the minimum acceptable configuration. For example, a computer that cannot run a secure operating system because it has an old processor (such as a 100-megahertz [MHz] x86-based computer).

Use these groups to assign costs for implementing the solution on the computers that require upgrades.

Known, untrusted state

During the process of categorizing an organization's computers, you will identify some computers that cannot achieve trusted status for specific well-understood and well-defined reasons. These reasons might include the following types:

- **Financial.** The funding is not available to upgrade the hardware or software for this computer.
- **Political.** The computer must remain in an untrusted state because of a political or business situation that does not enable it to comply with the stated minimum security requirements of the organization. It is highly recommended that you contact the business owner or independent software vendor (ISV) for the computer to discuss the added value of server and domain isolation.
- **Functional.** The computer must run a nonsecure operating system or must operate in a nonsecure manner to perform its role. For example, the computer might be required to run an older operating system because a specific line of business application will only work on that operating system.

There can be multiple functional reasons for a computer to remain in the known untrusted state. The following list includes several examples of functional reasons that can lead to a classification of this state:

- **Computers that run unsupported versions of Windows.** This includes Windows Millennium Edition, Windows 98, Windows 95, or Windows NT. Computers that run these versions of the Windows operating system cannot be classified as trustworthy because these operating systems do not support the required security infrastructure. For example, although Windows NT does support a basic security infrastructure, it does not support "deny" ACLs on local resources, any way to ensure the confidentiality and integrity of network communications, smart cards for strong authentication, or centralized management of computer configurations (although limited central management of user configurations is supported).
- **Stand-alone computers.** Computers running any version of Windows that are configured as stand-alone computers or as members of a workgroup usually cannot achieve a trustworthy state. Although these computers fully support the minimum required basic security infrastructure, the required security management capabilities are unlikely to be available when the computer is not a part of a trusted domain.
- **Computers in an untrusted domain.** A computer that is a member of a domain that is not trusted by an organization's IT department cannot be classified as trusted. An untrusted domain is a domain that cannot provide the required security capabilities to its members. Although the operating systems of computers that are members of this untrusted domain might fully support the minimum required basic security infrastructure, the required security management capabilities cannot be fully guaranteed when computers are not in a trusted domain.

Unknown, untrusted state

The unknown, untrusted state should be considered the default state for all computers. Because computers in this state have a configuration that is unknown, you can assign no trust to them. All planning for computers in this state must assume that the computer is an unacceptable risk to the organization. Designers of the solution should strive to minimize the impact that the computers in this state can have on their organizations.

Capturing upgrade costs for current computers

The final step in this part of the process is to record the approximate cost of upgrading the computers to a point that they can participate in the server and domain isolation design. You must make several key decisions during the design phase of the project that require answers to the following questions:

- Does the computer meet the minimum hardware requirements necessary for isolation?
- Does the computer meet the minimum software requirements necessary for isolation?
- What configuration changes must be made to integrate this computer into the isolation solution?
- What is the projected cost or impact of making the proposed changes to enable the computer to achieve a trusted state?

By answering these questions, you can quickly determine the level of effort and approximate cost of bringing a particular computer or group of computers into the scope of the project. It is important to remember that the state of a computer is transitive, and that by performing the listed remedial actions you can change the state of a computer from untrusted to trusted. After you decide whether to place a computer in a trusted state, you are ready to begin planning and designing the isolation groups, which the next section Planning Domain Isolation Zones discusses.

The following table is an example of a data sheet that you could use to help capture the current state of a computer and what would be required for the computer to achieve a trusted state.

Computer name	Hardware reqs met	Software reqs met	Configuration required	Details	Projected cost
CLIENT001	No	No	Upgrade hardware and software.	Current operating system is Windows 2000. Old hardware is not compatible with Windows Vista.	$??
SERVER001	Yes	No	Join trusted domain and upgrade from Windows 2000 to Windows Server 2008.	No antivirus software present.	$??

In the previous table, the computer CLIENT001 is currently "known, untrusted" because its hardware must be upgraded. However, it could be considered trustworthy if the required upgrades are possible. However, if many computers require the same upgrades, the overall cost of the solution would be much higher.

The computer SERVER001 is "trustworthy" because it meets the hardware requirements but its operating system must be upgraded. It also requires antivirus software. The projected cost is the amount of effort that is required to upgrade the operating system and install antivirus software, along with their purchase costs.

With the other information that you have gathered in this section, this information will be the foundation of the efforts performed later in the Planning Domain Isolation Zones section.

The costs identified in this section only capture the projected cost of the computer upgrades. Many additional design, support, test, and training costs should be accounted for in the overall project plan.

For more information about how to configure firewalls to support IPsec, see "Configuring Firewalls" at http://go.microsoft.com/fwlink/?linkid=69783.

For more information about WMI, see "Windows Management Instrumentation" at http://go.microsoft.com/fwlink/?linkid=110483.

Next: Planning Your Windows Firewall with Advanced Security Design

Planning Your Windows Firewall with Advanced Security Design

After you have gathered the relevant information in the previous sections, and understand the basics of the designs as described earlier in this guide, you can select the design (or combination of designs) that meet your needs.

Basic firewall design

We recommend that you deploy at least the basic firewall design. As discussed in the Protect Computers from Unwanted Network Traffic section, host-based firewalls are an important element in a defense-in-depth strategy and complement most other security measures you put in place in your organization.

When you are ready to examine the options for firewall policy settings, see the Planning Settings for a Basic Firewall Policy section.

Domain isolation design

Include this design in your plans if:

- You have an Active Directory domain of which most of the computers are members
- You want to prevent the computers in your organization from accepting any unsolicited network traffic from computers that are not part of the domain.

If you plan on including the basic firewall design as part of your deployment, we recommend that you deploy the firewall policies first to confirm that they work properly. Also plan to enable your connection security rules in request mode at first, instead of the more restrictive require mode, until you are sure that the computers are all correctly protecting network traffic with IPsec. If something is wrong, request mode still allows communications to continue while you are troubleshooting.

When you are ready to examine the options for creating an isolated domain, see the Planning Domain Isolation Zones section.

Server isolation design

Include this design in your plans:

- If you have an isolated domain and you want to additionally restrict access to specific servers to only authorized users and computers.
- You are not deploying an isolated domain, but want to take advantage of similar benefits for a few specific servers. You can restrict access to the isolated servers to only authorized users and computers.

If you plan to include domain isolation in your deployment, we recommend that you complete that layer and confirm its correct operation before you implement the additional server isolation elements.

When you are ready to examine the options for isolating servers, see the Planning Server Isolation Zones section.

Certificate-based authentication design

Include this design in your plans:

- If you want to implement some of the elements of domain or server isolation on computers that are not joined to an Active Directory domain, or do not want to use domain membership as an authentication mechanism.
- You have an isolated domain and want to effectively a server that is not a member of the Active Directory domain because the computer is not running Windows, or for any other reason.
- You must enable external computers that are not managed by your organization to access information on one of your servers, and want to do this in a secure way.

If you plan to include domain or server isolation in your deployment, we recommend that you complete those elements and confirm their correct operation before you add certificate-based authentication to the computers that require it.

When you are ready to examine the options for using certificate-based authentication, see the Planning Certificate-based Authentication section.

Documenting your design

After you finish selecting the designs that you will use, you must assign each of your computers to the appropriate isolation zone and document the assignment for use by the deployment team.

- Documenting the Zones

Designing groups and GPOs

After you have selected a design and assigned your computers to zones, you can begin laying out the isolation groups for each zone, the network access groups for isolated server access, and the GPOs that you will use to apply the settings and rules to your computers.

When you are ready to examine the options for the groups, filters, and GPOs, see the Planning Group Policy Deployment for Your Isolation Zones section.

Next: Planning Settings for a Basic Firewall Policy

Planning Settings for a Basic Firewall Policy

After you have identified your requirements, and have the information about the network layout and computers available, you can begin to design the GPO settings and rules that will enable you to enforce your requirements on the computers.

The following is a list of the firewall settings that you might consider for inclusion in a basic firewall design, together with recommendations to serve as a starting point for your analysis:

- **Profile selection**. The firewall rules can be configured for any of the network location profiles that you see in the Network and Sharing Center: domain, public, and private (on Windows Vista and Windows Server 2008), or domain and standard (on Windows XP or Windows Server 2003). Most settings are enforced in the domain profile, without an option for the user to change them. However, you might want to leave the profile settings configurable by the user on computers that can be taken from the organization's physical network and joined to a public or home network. If you lock down the public and private profiles, you might prevent a user from accessing a required network program or service. Because they are not on the organization's network, you cannot fix a connectivity problem by deploying rule changes in a GPO. For each section that follows, consider each profile and apply the rules to those profiles that make sense for your organization.

Important

By default, a new network adapter installed in a computer is set as a public network connection and, if not configured for a different profile, might automatically switch the computer to public profile. We recommend that on server computers that you set all rules for all profiles to prevent any unexpected profile switch from disrupting network connectivity. You might consider a similar practice for your desktop computers, and only support different profiles on portable computers.

- **Firewall state: On**. We recommend that you turn the firewall on, and prevent the user from turning it off.
- **Default behavior for Inbound connections: Block**. We recommend that you enforce the default behavior of blocking unsolicited inbound connections. To allow network traffic for a specific program, create an inbound rule that serves as an exception to this default behavior.
- **Default behavior for Outbound connections: Allow**. We recommend that you enforce the default behavior of allowing outbound connections. Create outbound block rules to prevent the traffic that you know must be blocked.

- **Display a notification: Yes** (for client computers), **No** (for server computers). We recommend that you allow the client computers to display a message to the user when the firewall blocks a program. This enables the user to select whether to allow the program to listen. If the user allows the program, then Windows automatically creates a new inbound rule for the program. The user can do this only if the user's account is a member of the Administrators group, or if the user can supply administrator account credentials to the User Account Control dialog box.

If set to **No**, you must ensure that all programs required by the computer can successfully communicate on the network as needed, either by using the default firewall behavior, or by creating an inbound firewall rule for the program.

On servers, we recommend that you turn the notification off, because typically no administrators are waiting to respond if a notification is displayed. In addition, the server roles included with Windows Server 2008 create and enable appropriate rules when you install the role. For example, if you install the Active Directory Domain Controller role, a variety of rules to allow inbound network traffic for Active Directory services are created and enabled for all network location profiles.

When this setting is set to **No**, then the **Apply local firewall rules setting** is typically set to **No** also.

- **Allow unicast response: Yes**. We recommend that you use the default setting of **Yes** unless you have specific requirements to do otherwise.

- **Apply local firewall rules: Yes**. We recommend that you allow users to create and use local firewall rules. If you set this to **No**, then when a user clicks **Allow** on the notification message to allow traffic for a new program, Windows does not create a new firewall rule and the traffic remains blocked.

If you and the IT staff can create and maintain the list of firewall rules for all permitted applications and deploy them by using GPOs then you can set this value to **No**.

- **Apply local connection security rules: No**. We recommend that you prevent users from creating and using their own connection security rules. Connection failures caused by conflicting rules can be difficult to troubleshoot.

- **Logging**. We recommend that you enable logging to a file on the local hard disk. Be sure to limit the size, such as 4096 KB, to avoid causing performance problems by filling the user's hard disk. Be sure to specify a folder to which the Windows Firewall service account has write permissions.

- **Inbound rules**. Create inbound rules for programs that must be able to receive unsolicited inbound network packets from another computer on the network. Make the rules as specific as possible to reduce the risk of malicious programs exploiting the rules. For example, specify both program and port numbers. Specifying a program ensures that the rule is only active when the program is actually running, and specifying the port number ensures that the program cannot receive unexpected traffic on a different port.

Inbound rules are common on servers, because they host services to which client computers connect. When you install programs and services on a server, the installation program typically creates and enables the rules for you. Examine the rules to ensure that they do not open up more ports than are required.

Important

If you create inbound rules that permit RPC network traffic by using the **RPC Endpoint Mapper** and **Dynamic RPC** rule options, then all inbound RPC network traffic is permitted because the firewall cannot filter network traffic based on the UUID of the destination application.

- **Outbound rules**. Only create outbound rules to block network traffic that must be prevented in all cases. If your organization prohibits the use of certain network programs, you can support that policy by blocking the known network traffic used by the program. Be sure to test the restrictions before you deploy them to avoid interfering with traffic for needed and authorized programs.

Next: Planning Domain Isolation Zones

Planning Domain Isolation Zones

After you have the required information about your network, Active Directory, and client and server computers, you can use that information to make decisions about the isolation zones you want to use in your environment.

The bulk of the work in planning server and domain isolation is determining which computers to assign to each isolation zone. Correctly choosing the zone for each computer is important to providing the correct level of security without compromising performance or the ability a computer to send or receive required network traffic.

The zones described in this guide include the following:

- Exemption List
- Isolated Domain
- Boundary Zone
- Encryption Zone

Exemption List

When you implement a server and domain isolation security model in your organization, you are likely to find some additional challenges. Key infrastructure servers such as DNS servers, and DHCP servers typically must be available to all computers on the internal network, yet secured from network attacks. However, if they must remain available to all computers on the network, not just to isolated domain members, then these servers cannot require IPsec for inbound access, nor can they use IPsec transport mode for outbound traffic.

Some services, such as DNS, do not work well with the **Fall back to clear** setting when one of the computers takes three-seconds between a failed IKE attempt and the follow-up plaintext attempt. This delay causes performance and time-out errors for many services as noted above. The "Simple Policy Update" for Windows XP with SP2 and Windows Server 2003 with SP1 (available at http://go.microsoft.com/fwlink/?linkid=110514) reduces the delay to one-half second.

Later service packs for both Windows XP and Windows Server 2003have the update built-in. For many services, this reduction in the delay means that the services do not require exemption. This is a key means to keep the size of the exemption list as small as possible.

With Windows Vista and Windows Server 2008, the delay is eliminated. When **Fall back to clear** is specified, both IPsec and plaintext connection attempts are made at the same time. If the remote computer responds to the IPsec request, then the plaintext attempt is abandoned. If the remote computer does not respond to the IPsec request then the plaintext attempt is permitted to proceed, and the IPsec request eventually times out.

However, if you have any computers in your organization that are running operating systems that cannot run the Simple Policy Update, then you must maintain a comprehensive exemption list.

In addition to the infrastructure servers mention earlier, there might also be other servers on the network that trusted computers cannot use IPsec to access, which would be added to the exemption list.

Generally, the following conditions are reasons to consider adding a computer to the exemption list:

- If the computer must be accessed by trusted computers but it does not have a compatible IPsec implementation.
- If the computer must provide services to both trusted and untrusted computers, but does not meet the criteria for membership in the boundary zone.
- If the computer must run a program that is adversely affected by IPsec encapsulation of program traffic.
- If the computer must support so many clients at the same time and you find that IPsec causes an unacceptable drop in performance.
- If the computer must be accessed by trusted computers from different isolated domains that do not have an Active Directory trust relationship established with each other.
- If the computer is a domain controller running an earlier version of Windows than Windows Server 2008, or if any of its clients are running an earlier version of Windows than Windows Vista.
- If the computer must support trusted and untrusted computers, but cannot use IPsec to help secure communications to trusted computers.

For large organizations, the list of exemptions might grow very large if all the exemptions are implemented by one connection security rule for the whole domain or for all trusted forests. If you can require all computers in your isolated domain to run at least Windows XP with SP2 or Windows Server 2003 with SP1 with the Simple Policy Update, you can greatly reduce the size of this list. A large exemption list has several unwanted effects on every computer that receives the GPO, including the following:

- Reduces the overall effectiveness of isolation.
- Creates a larger management burden (because of frequent updates).

- Increases the size of the IPsec policy, which means that it consumes more memory and CPU resources, slows down network throughput, and increases the time require to download and apply the GPO containing the IPsec policy.

To keep the number of exemptions as small as possible, several options exist:

- Carefully consider the communications requirements of each isolation zone, especially server-only zones. They might not be required to communicate with every exemption in the domain-level policy for clients.
- Consolidate server functions. If several exempt services can be hosted at one IP address, the number of exemptions is reduced.
- Consolidate exempted hosts on the same subnet. Where network traffic volume allows, you might be able to locate the servers on a subnet that is exempted, instead of using exemptions for each IP address.

As with defining the boundary zone, create a formal process to approve hosts being added to the exemption list. For a model for processing requests for exemptions, see the decision flowchart in the Boundary Zone section.

Next: Isolated Domain

Isolated Domain

The isolated domain is the primary zone for trusted computers. The computers in this zone use connection security and firewall rules to control the communications that can be sent between computers in the zone.

The term *domain* in this context means a boundary of communications trust instead of an Active Directory domain. In this solution the two constructs are very similar because Active Directory domain authentication (Kerberos V5) is required for accepting inbound connections from trusted computers. However, many Active Directory domains (or forests) can be linked with trust relationships to provide a single, logical, isolated domain. In addition, computers that authenticate by using certificates can also be included in an isolated domain without joining the Active Directory domain.

For most implementations, an isolated domain will contain the largest number of computers. Other isolation zones can be created for the solution if their communication requirements differ from those of the isolated domain. Examples of these differences are what result in the boundary and encryption zones described in this guide. Conceptually, the isolated domain is just the largest isolation zone, and a superset to the other zones.

You must create a group in Active Directory to contain members of the isolated domain. You then apply one of several GPOs that contain connection security and firewall rules to the group so that authentication on all inbound network connections is enforced. Creation of the group and how to link the GPOs that apply the rules to its members are discussed in the Planning Group Policy Deployment for Your Isolation Zones section.

The GPOs for the isolated domain should contain the following connection security rules and settings.

GPO settings for isolated domain members running Windows Vista or Windows Server 2008

GPOs for computers running Windows Vista or Windows Server 2008 should include the following:

- IPsec default settings that specify the following options:

  a. Exempt all ICMP traffic from IPsec.

  b. Key exchange (main mode) security methods and algorithm. We recommend that you do not include Diffie-Hellman Group 1, Data Encryption Standard (DES), or MD5 in any setting. They are included only for compatibility with earlier versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

  c. Data protection (quick mode) algorithm combinations. We recommend that you do not include DES, or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

  If any NAT devices are present on your networks, do not use AH because it cannot traverse NAT devices. If isolated domain members must communicate with hosts in the encryption zone, ensure that you include algorithms that are compatible with the requirements of the encryption mode policies.

  d. Authentication methods. Include at least computer-based Kerberos V5 authentication. If you want to use user-based access to isolated servers, then also include user-based Kerberos V5 as an optional authentication method. Likewise, if any of your isolated domain members cannot use Kerberos V5 authentication, then include certificate-based authentication as an optional authentication method.

- A connection security rule that exempts all computers on the exemption list from authentication. Be sure to include all your Active Directory domain controllers on this list. Enter subnet addresses, where possible, instead of discrete addresses, if applicable in your environment.

- A connection security rule, from any IP address to any, that requires inbound and requests outbound authentication by using Kerberos V5 authentication.

Important

Be sure to begin operations by using request in and request out behavior until you are sure that all the computers in your IPsec environment are communicating successfully by using IPsec. After confirming that IPsec is operating as expected, you can change the policy to require in, request out.

GPO settings for isolated domain members running Windows 2000, Windows Server 2003, or Windows XP

GPOs for computers running Windows 2000, Windows Server 2003, or Windows XP should include the following:

- An IPsec Policy that includes the following settings and security rules:

a. Key exchange settings that specify main mode security methods and algorithms. We recommend that you do not include Diffie-Hellman Group 1, DES, or MD5 in any setting. They are included only for compatibility with previous versions of Windows. You should use the strongest algorithm combinations that are common to all your supported operating systems.

b. A permit rule for all ICMP traffic using **My IP Address** to **Any IP Address**.

c. A permit rule for all computers on the exemption list. Be sure to include all your Active Directory domain controllers on this list. Take advantage of the ability to enter subnet addresses, if applicable in your environment.

d. A negotiate rule for all network addresses using **My IP Address** to communicate with subnet addresses that make up the network address space. The filter action should specify **Negotiate security**, and then specify the same integrity and encryption protocols that are used by your other computers. We recommend that you do not include DES, or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems. If any NAT devices are present on your networks, do not use AH because it cannot traverse NAT devices.

To initially make the IPsec policy request authentication for both inbound and outbound traffic, select both **Accept unsecured communication** and **Allow fallback to unsecured communication** check boxes. After you have confirmed that all your computers are successfully using IPsec as designed, come back to this setting, and then clear the **Accept unsecured communication** check box to require inbound authentication.

- A registry policy that includes the following values:

  a. Set the **IPsec Default Exemptions** registry entry to a value of **2** to exempt only Resource Reservation Protocol (RSVP), Kerberos V5, and ISAKMP. This setting is documented in Knowledge Base article 810207 at http://go.microsoft.com/fwlink/?linkid=110516.

  b. Set the **Simplified IPsec Policy** registry entry to a value of **0x14** to improve the 'fall back to clear' behavior in Windows XP and Windows Server 2003. To use this, you must have already deployed the update available for free download (for Windows Server 2003) from the Knowledge Base article 914841 at http://go.microsoft.com/fwlink/?linkid=110514.

For a sample template for these registry settings, see Appendix A: Sample GPO Template File for Settings Used in this Guide.

For more information about how to create .adm files for use with Windows Group Policy, see http://go.microsoft.com/fwlink/?linkid=110517.

Make sure that in your GPOs for stationary computers, such as desktop and server computers, assign all rules to all profiles. For portable computers, you might want to allow more profile flexibility to enable users to communicate successfully when they are not connected to the organization's network.

Next: Boundary Zone

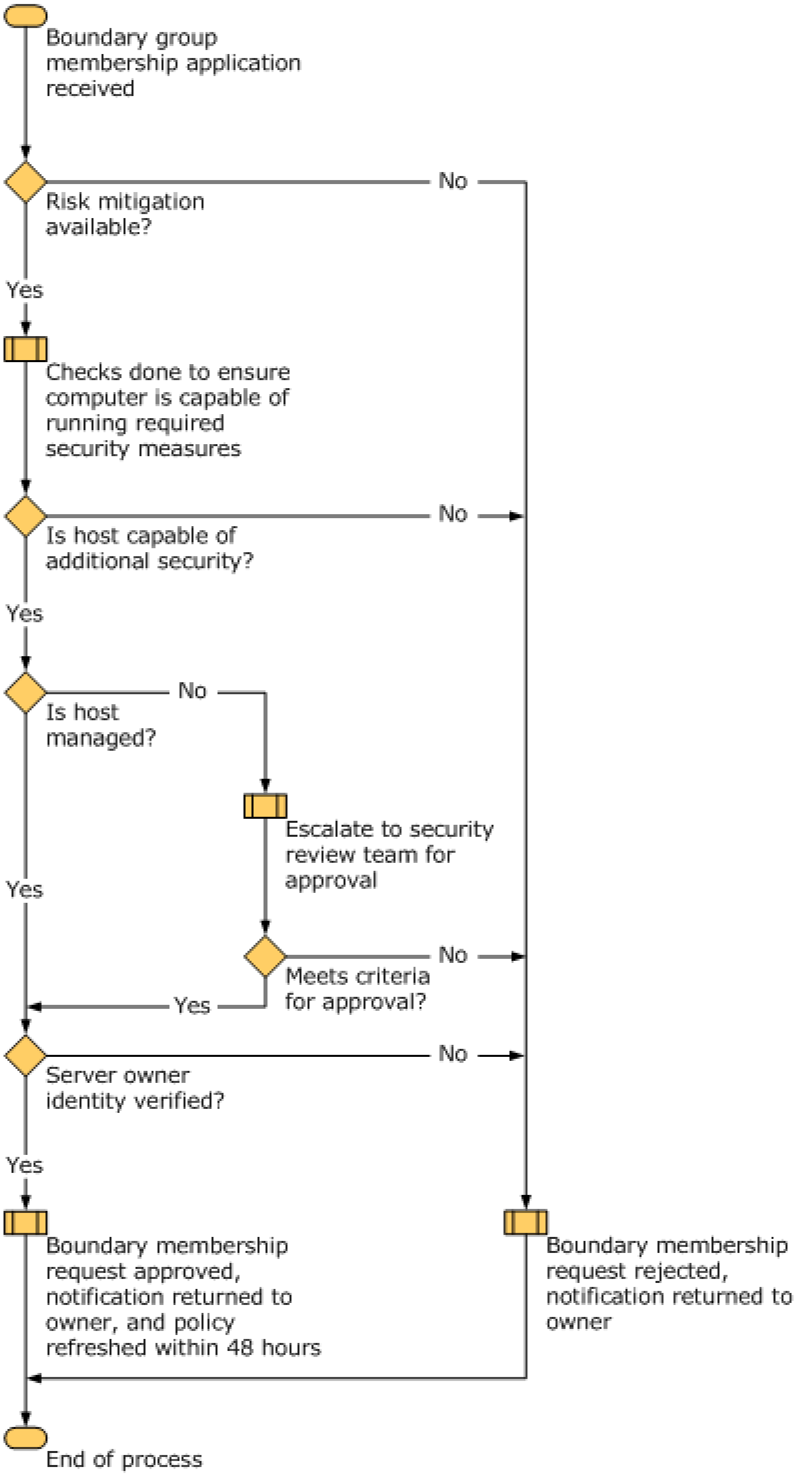
Boundary Zone

In most organizations, some computers must be able to receive network traffic from computers that are not part of the isolated domain, and therefore cannot authenticate. To accept communications from untrusted computers, create a boundary zone within your isolated domain. .

Computers in the boundary zone are trusted computers that can accept communication requests both from other isolated domain member computers and from untrusted computers. Boundary zone computers try to authenticate any incoming request by using IPsec, initiating an IKE negotiation with the originating computer. However, if no IKE response is received, the computer will "fall back to clear" and begin communicating in plaintext without IPsec.

The GPOs you build for the boundary zone include IPsec or connection security rules that request authentication for both inbound and outbound network connections, but do not require it.

Because these boundary zone computers can receive unsolicited inbound communications from untrusted computers that use plaintext, they must be carefully managed and secured in other ways. Mitigating this additional risk is an important part of deciding whether to add a computer to the boundary zone. For example, completing a formal business justification process before adding each computer to the boundary zone can help ensure that the additional risk is minimized. The following illustration shows a sample process that can help make such a decision.


Boundary group membership application received
Risk mitigation available?
No
Yes
Checks done to ensure computer is capable of running required security measures
Is host capable of additional security?
No
Yes
Is host managed?
No
Escalate to security review team for approval
Yes
Meets criteria for approval?
No
Yes
Server owner identity verified?
No
Yes
Boundary membership request approved, notification returned to owner, and policy refreshed within 48 hours
Boundary membership request rejected, notification returned to owner
End of process

The goal of this process is to determine whether the risk of adding a computer to a boundary zone can be mitigated to a level that makes it acceptable to the organization. Ultimately, if the risk cannot be mitigated, membership must be denied.

You must create a group in Active Directory to contain the members of the boundary zones. The settings and rules for the boundary zone are typically very similar to those for the isolated domain, and you can save time and effort by copying those GPOs to serve as a starting point. The primary difference is that the authentication connection security rule must be set to request authentication for both inbound and outbound traffic, instead of requiring inbound authentication and requesting outbound authentication as used by the isolated domain.

Creation of the group and how to link it to the GPOs that apply the rules to members of the group are discussed in the Planning Group Policy Deployment for Your Isolation Zones section.

GPO settings for boundary zone servers running Windows Server 2008

The boundary zone GPO for computers running Windows Server 2008 should include the following:

- IPsec default settings that specify the following options:

  a. Exempt all ICMP traffic from IPsec.

  b. Key exchange (main mode) security methods and algorithm. We recommend that you do not include Diffie-Hellman Group 1, DES, or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

  c. Data protection (quick mode) algorithm combinations. We recommend that you do not include DES or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems. If any NAT devices are present on your networks, do not use AH because it cannot traverse NAT devices. If these computers must communicate with hosts in the encryption zone, ensure that you include an algorithm that is compatible with the requirements of the encryption zone GPOs.

  d. Authentication methods. Include at least computer-based Kerberos V5 authentication. If you want to use user-based access to isolated servers then you must also include user-based Kerberos V5 authentication as an optional authentication method. Likewise, if any of your domain isolation members cannot use Kerberos V5, you must include certificate-based authentication as an optional authentication method.

- A connection security rule that exempts all computers on the exemption list from authentication. Be sure to include all your Active Directory domain controllers on this list. Enter subnet addresses, if applicable in your environment.

- A connection security rule, from **Any IP address** to **Any IP address**, that requests inbound and outbound authentication.

GPO settings for boundary zone servers running Windows 2000 or Windows Server 2003

You must create a new IPsec policy instead of modifying an existing IPsec policy in a copied GPO. Because all GPOs share a common store of IPsec policies, if you modify an IPsec policy in a copied GPO, you are modifying the shared one used by other GPOs. Make sure that your newly created IPsec policy is the one assigned in the GPO.

The GPOs for computers that are running Windows 2000 or Windows Server 2003 should include the following:

- An IPsec policy that includes the following settings and security rules:

    a. Key exchange settings that specify main mode security methods and algorithms. We recommend that you do not include Diffie-Hellman Group 1, DES, or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

    b. A permit rule for all ICMP traffic using **My IP Address** to **Any IP Address**.

    c. A permit rule for all computers on the exempted list. Be sure to include all your Active Directory domain controllers on this list. Take advantage of the ability to enter subnet addresses, if applicable in your environment.

    d. A negotiate rule for all network addresses using **My IP Address** to communicate with subnet addresses that make up the network address space. The filter action should specify **Negotiate security**, and then specify the same integrity and encryption protocols that are used by your other computers. We recommend that you do not include DES or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems. If any NAT devices are present on your networks, do not use AH because it cannot traverse NAT devices.

  To make the policy request authentication for inbound and outbound traffic, select both of the **Accept unsecured communication** and **Allow fallback to unsecured communication** check boxes.

- A registry policy that includes the following values:

    a. Set the **IPsec Default Exemptions** registry entry to a value of **2** to exempt only RSVP, Kerberos, and ISAKMP. This setting is documented in Knowledge Base article 810207 at http://go.microsoft.com/fwlink/?linkid=110516.

    b. Set the **Simplified IPsec Policy** registry entry to a value of **0x14** to improve the 'fall back to clear' behavior in Windows XP and Windows Server 2003. To use this, you must have already deployed the update available for free download (for Windows Server 2003) from the Knowledge Base article 914841 at http://go.microsoft.com/fwlink/?linkid=110514.

For a sample template for these registry settings, see Appendix A: Sample GPO Template File for Settings Used in this Guide.

For more information about how to create .adm files for use with Windows Group Policy, see Using Administrative Template Files with Registry-Based Group Policy at http://go.microsoft.com/fwlink/?linkid=110517.

Make sure that your GPOs for stationary computers, such as desktop and server computers, assign all rules to all profiles. For portable computers, you might want to allow more profile flexibility to enable users to communicate successfully when they are not connected to the organization's network.

Next: Encryption Zone

Encryption Zone

Some servers in the organization host data that is very sensitive, including medical, financial, or other personally identifying data. Government or industry regulations might require that this sensitive information must be encrypted when it is transferred between computers.

To support the additional security requirements of these servers, we recommend that you create an encryption zone to contain the computers and that requires that the sensitive inbound and outbound network traffic be encrypted.

You must create a group in Active Directory to contain members of the encryption zone. The settings and rules for the encryption zone are typically similar to those for the isolated domain, and you can save time and effort by copying those GPOs to serve as a starting point. You then modify the security methods list to include only algorithm combinations that include encryption protocols.

Creation of the group and how to link it to the GPOs that apply the rules to members of the group are discussed in the Planning Group Policy Deployment for Your Isolation Zones section.

GPO settings for encryption zone servers running Windows Server 2008

The GPO for computers that are running Windows Server 2008 should include the following:

- IPsec default settings that specify the following options:

    a. Exempt all ICMP traffic from IPsec.

    b. Key exchange (main mode) security methods and algorithm. We recommend that you do not include Diffie-Hellman Group 1, DES, or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

    c. Data protection (quick mode) algorithm combinations. Check **Require encryption for all connection security rules that use these settings**, and then specify one or more integrity and encryption combinations. We recommend that you do not include DES or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

  If any NAT devices are present on your networks, do not use AH because it cannot traverse NAT devices.

    d. Authentication methods. Include at least computer-based Kerberos V5 authentication. If you want to use user-based access to isolated servers then you must also include user-based Kerberos V5 authentication as an optional authentication method. Likewise, if any of your domain isolation members cannot use Kerberos V5 authentication, then you must include certificate-based authentication as an optional authentication method.

- A connection security rule that exempts all computers on the exemption list from authentication. Be sure to include all your Active Directory domain controllers on this list. Enter subnet addresses, if applicable in your environment.
- A connection security rule, from any IP address to any, that requires inbound and requests outbound authentication using the default authentication specified earlier in this policy.

Important

Be sure to begin operations by using request in and request out behavior until you are sure that all the computers in your IPsec environment are communicating successfully by using IPsec. After confirming that IPsec is operating as expected, you can change the GPO to require in, request out.

- If domain member computers must communicate with computers in the encryption zone, ensure that you include in the isolated domain GPOs quick mode combinations that are compatible with the requirements of the encryption zone GPOs.

GPO settings for encryption zone servers running Windows 2000 or Windows Server 2003

You must create a new IPsec policy instead of modifying an existing IPsec policy in a copied GPO. Because all GPOs share a common store of IPsec policies, if you modify an IPsec policy in a copied GPO, you are modifying the shared one used by other GPOs. Make sure that your newly created IPsec policy is the one assigned in the GPO.

The GPOs for computers that are running Windows 2000 or Windows Server 2003 should include the following:

- An IPsec policy that includes the following settings and security rules:

  a. Key exchange settings that specify main mode security methods and algorithms. We recommend that you do not include Diffie-Hellman Group 1, DES, or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

  b. A permit rule for all ICMP traffic using **My IP Address** to **Any IP Address**.

  c. A permit rule for all computers on the exempted list. Be sure to include all your Active Directory domain controllers on this list. Take advantage of the ability to enter subnet addresses, if applicable in your environment.

  d. A negotiate rule for all network addresses using **My IP Address** to communicate with subnet addresses that make up the network address space. The filter action should specify **Negotiate security** and then specify the encryption protocols to be required by members of the zone. We recommend that you do not include DES or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems. If any

NAT devices are present on your networks, do not use AH because it cannot traverse NAT devices.

To initially make the GPO request inbound and outbound authentication, select both the **Accept unsecured communication** and **Allow fallback to unsecured communication** check boxes. After you have confirmed that all your computers are successfully using IPsec as designed, come back to this setting, and then clear the **Accept unsecured communication** check box to require inbound authentication.

- A registry policy that includes the following values:

  a. Set the **IPsec Default Exemptions** registry entry to a value of **2** to exempt only RSVP, Kerberos V5, and ISAKMP. This setting is documented in Knowledge Base article 810207 at http://go.microsoft.com/fwlink/?linkid=110516.

  b. Set the **Simplified IPsec Policy** registry entry to a value of **0x14** to improve the 'fall back to clear' behavior in Windows XP and Windows Server 2003. To use this, you must have already deployed the update available for free download (for Windows Server 2003) from the Knowledge Base article 914841 at http://go.microsoft.com/fwlink/?linkid=110514.

For a sample template for these registry settings, see Appendix A: Sample GPO Template File for Settings Used in this Guide.

For more information about how to create .adm files for use with Windows Group Policy, see http://go.microsoft.com/fwlink/?linkid=110517.

Make sure that your GPOs for stationary computers, such as desktop and server computers, assign all rules to all profiles. For portable computers, you might want to allow more profile flexibility to enable users to communicate successfully when they are not connected to the organization's network.

Next: Planning Server Isolation Zones

Planning Server Isolation Zones

Sometimes a server hosts data that is sensitive. If your servers host data that must not be compromised, you have several options to help protect that data. One was already addressed: adding the server to the encryption zone. Membership in that zone prevents the server from being accessed by any computers that are outside the isolated domain, and encrypts all network connections to server.

The second option is to additionally restrict access to the server, not just to members of the isolated domain, but to only those users or computers who have business reasons to access the resources on the server. You can specify only approved users, or you can additionally specify that the approved users can only access the server from approved computers.

To grant access, you add the approved user and computer accounts to network access groups (NAGs) that are referenced in a firewall rule on this server. When the user sends a request to the server, the standard domain isolation rules are invoked. This causes IKE to use Kerberos V5 to exchange credentials with the server. The additional firewall rule on the server causes Windows to check the provided computer and user accounts for group membership in the NAGs. If either the user or computer is not a member of a required NAG then the network connection is refused.

Isolated domains and isolated servers

If you are using an isolated domain, the client computers already have the IPsec rules to enable them to authenticate traffic when the server requires it. If you add an isolated server, it must have a GPO applied to its group with the appropriate connection security and firewall rules. The rules enforce authentication and restrict access to only connections that are authenticated as coming from an authorized computer or user.

If you are not using an isolated domain, but still want to isolate a server that uses IPsec, you must configure the client computers that you want to access the server to use the appropriate IPsec rules. If the client computers are members of an Active Directory domain, you can still use Group Policy to configure the clients. Instead of applying the GPO to the whole domain, you apply the GPO to only members of the NAG.

Creating multiple isolated server zones

Each set of servers that must be accessed by different sets of users should be set up in its own isolated server zone. After one set of GPOs for one isolated server zone has been successfully created and verified, you can copy the GPOs to a new set. You must change the GPO names to reflect the new zone, the name and membership of the isolated server zone group to which the GPOs are applied, and the names and membership of the NAG groups that determine which clients can access the servers in the isolated server zone.

Creating the GPOs

Creation of the groups and how to link them to the GPOs that apply the rules to members of the groups are discussed in the Planning Group Policy Deployment for Your Isolation Zones section.

An isolated server is often a member of the encryption zone. Therefore, copying that GPO set serves as a good starting point. You then modify the rules to additionally restrict access to only NAG members.

GPO settings for isolated servers running Windows Server 2008

GPOs for computers running Windows Server 2008 should include the following:

Note

> The connection security rules described here are identical to the ones for the encryption zone. If you do not want to encrypt access and also restrict access to NAG members, you can use connection security rules identical to the main isolated domain. You must still add the firewall rule described at the end of this list to change it into an isolated server zone.

- IPsec default settings that specify the following options:

  a. Exempt all ICMP traffic from IPsec.

  b. Key exchange (main mode) security methods and algorithm. We recommend that you do not include Diffie-Hellman Group 1, DES, or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

c. Data protection (quick mode) algorithm combinations. Check **Require encryption for all connection security rules that use these settings**, and then specify one or more integrity and encryption combinations. We recommend that you do not include DES or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

If any NAT devices are present on your networks, do not use AH because it cannot traverse NAT devices. If isolated servers must communicate with hosts in the encryption zone, include an algorithm that is compatible with the requirements of the encryption zone GPOs.

d. Authentication methods. Include at least computer-based Kerberos V5 authentication for compatibility with the rest of the isolated domain. If you want to restrict access to specific user accounts, also include user-based Kerberos V5 authentication as an optional authentication method. Do not make the user-based authentication method mandatory, or else computers that cannot use AuthIP instead of IKE, including Windows XP and Windows Server 2003, cannot communicate. Likewise, if any of your domain isolation members cannot use Kerberos V5, include certificate-based authentication as an optional authentication method.

- A connection security rule that exempts all computers on the exemption list from authentication. Be sure to include all your Active Directory domain controllers on this list. Enter subnet addresses, if applicable in your environment.
- A connection security rule, from **Any IP address** to **Any IP address**, that requires inbound and requests outbound authentication by using Kerberos V5 authentication.

Important

Be sure to begin operations by using request in and request out behavior until you are sure that all the computers in your IPsec environment are communicating successfully by using IPsec. After confirming that IPsec is operating as expected, you can change the GPO to require in, request out.

- A firewall rule that specifies **Allow only secure connections**, **Require encryption**, and on the **Users and Computers** tab includes references to both computer and user network access groups.

GPO settings for isolated servers running Windows 2000 or Windows Server 2003

You must create a new IPsec policy instead of modifying an existing IPsec policy in a copied GPO. Because all GPOs share a common store of IPsec policies, if you modify an IPsec policy in a copied GPO, you are modifying the shared one used by other GPOs. Make sure that your newly created IPsec policy is the one assigned in the GPO.

The GPOs for computers that are running Windows 2000 or Windows Server 2003 should include the following:

Note

This IPsec policy is identical to the one for the encryption zone setting, except for the addition of the User Rights Assignment setting. If you do not want to encrypt access and also restrict access to NAG members, you can use an IPsec policy identical to the main isolated domain.

- An IPsec policy that includes the following settings and security rules:

    a. Key exchange settings that specify main mode security methods and algorithms. We recommend that you do not include Diffie-Hellman Group 1, DES, or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems.

    b. A permit rule for all ICMP traffic using **My IP Address** to **Any IP Address**.

    c. A permit rule for all computers on the exempted list. Be sure to include all your Active Directory domain controllers on this list. Take advantage of the ability to enter subnet addresses, if applicable in your environment.

    d. A negotiate rule for all network addresses using **My IP Address** to subnet addresses that make up the network address space. The filter action should specify **Negotiate security**, and then specify the encryption protocols to be required by members of the zone. We recommend that you do not include DES or MD5 in any setting. They are included only for compatibility with previous versions of Windows. Use the strongest algorithm combinations that are common to all your supported operating systems. If any NAT devices are present on your networks, do not use AH because it cannot traverse NAT devices.

To initially make the GPO request authentication for inbound and outbound traffic, select both the **Accept unsecured communication** and **Allow fallback to unsecured communication** check boxes. After you have confirmed that all your computers are successfully using IPsec as designed, come back to this setting, and then clear the **Accept unsecured communication** check box to require inbound authentication.

- A User Rights Assignment setting that sets the **Access this computer from the network** user right to only include the computer NAG, the user NAG, and the IPsec exempt computers. Ensure that users who must administer the server, and the computers from which they work are members of the NAG groups.

- Also under User Rights Assignment, you can consider adding groups for users or computers that must be prevented from accessing the servers in the isolation zone. They are added to the **Deny access to this computer from the network** user right. This might include the CG_DOMISO_Boundary group, because they are computers at a greater risk of being compromised and therefore pose a higher risk to your isolated servers.

- A registry policy that includes the following values:

a. Set the **IPsec Default Exemptions** registry entry to a value of **2** to exempt only RSVP, Kerberos V5, and ISAKMP. This setting is documented in Knowledge Base article 810207 at http://go.microsoft.com/fwlink/?linkid=110516.

b. Set the **Simplified IPsec Policy** registry entry to a value of **0x14** to improve the 'fall back to clear' behavior in Windows XP and Windows Server 2003. To use this, you must have already deployed the update available for free download (for Windows Server 2003) from the Knowledge Base article 914841 at http://go.microsoft.com/fwlink/?linkid=110514.

For a sample template for these registry settings, see Appendix A: Sample GPO Template File for Settings Used in this Guide.

For more information about how to create .adm files for use with Windows Group Policy, see http://go.microsoft.com/fwlink/?linkid=110517.

Make sure that your GPOs for stationary computers, such as desktop and server computers, assign all rules to all profiles. For portable computers, you might want to allow more profile to enable users to communicate successfully when they are not connected to the organization's network.

Next: Planning Certificate-based Authentication

Planning Certificate-based Authentication

Sometimes a computer cannot join an Active Directory domain, and therefore cannot use Kerberos V5 authentication with domain credentials. However, the computer can still participate in the isolated domain by using certificate-based authentication.

The non-domain member server, and the clients that must be able to communicate with it, must be configured to use cryptographic certificates based on the X.509 standard. These certificates can be used as an alternate set of credentials. During IKE negotiation, each computer sends a copy of its certificate to the other computer. Each computer examines the received certificate, and then validates its authenticity. To be considered authentic, the received certificate must be validated by a certification authority certificate in the recipient's Trusted Root Certification Authorities store on the local computer.

Certificates can be acquired from commercial firms, or by an internal certificate server set up as part of the organization's public key infrastructure (PKI). Microsoft provides a complete PKI and certification authority solution with Windows Server 2008, Active Directory Certificate Services (AD CS). For more information about creating and maintaining a PKI in your organization, see Active Directory Certificate Services at http://go.microsoft.com/fwlink/?linkid=110820.

Deploying certificates

However you acquire your certificates, you must deploy them to your clients and servers that require them in order to communicate.

Using Active Directory Certificate Services

If you use AD CS to create your own user and computer certificates in-house, then the servers designated as certification authorities (CAs) create the certificates based on administrator-designed templates. AD CS then uses Group Policy to deploy the certificates to domain member computers. Computer certificates are deployed when a domain member computer starts. User certificates are deployed when a user logs on.

If you want non-domain member computers to be part of a server isolation zone that requires access by only authorized users, make sure to include certificate mapping to associate the certificates with specific user accounts. When certificate mapping is enabled, the certificate issued to each computer or user includes enough identification information to enable IPsec to match the certificate to both user and computer accounts.

AD CS automatically ensures that certificates issued by the CAs are trusted by the client computers by putting the CA certificates in the appropriate store on each domain member computer.

Using a commercially purchased certificate for computers running Windows

You can import the certificates manually onto each computer if the number of computers is relatively small. For a deployment to more than a handful of computers, use Group Policy.

You must first download the vendor's root CA certificate, and then import it to a GPO that deploys it to the Local Computer\Trusted Root Certification Authorities store on each computer that applies the GPO.

You must also import the purchased certificate into a GPO that deploys it to the Local Computer\Personal store on each computer that applies the GPO.

Using a commercially purchased certificate for computers running a non-Windows operating system

If you are installing the certificates on an operating system other than Windows, see the documentation for that operating system.

Configuring IPsec to use the certificates

Once the clients and servers have the certificates available, you can configure the IPsec and connection security rules to include those certificates as a valid authentication method. The authentication method requires the subject name of the certificate, for example: **DC=com,DC=woodgrovebank,CN=CorporateCertServer**. Optionally, select **Enable certificate to account mapping** to support using these credentials for restricting access to users or computers that are members of authorized groups in a server isolation solution.

Next: Documenting the Zones

Documenting the Zones

Generally, the task of determining zone membership is not complex, but it can be time-consuming. Use the information generated during the Designing a Windows Firewall with Advanced Security Strategy section of this guide to determine the zone in which to put each host. You can document this zone placement by adding a Group column to the inventory table shown in the Designing a Windows Firewall with Advanced Security Strategy section. A sample is shown here:

Host name	Hardware reqs met	Software reqs met	Configuration required	Details	Projected cost	Group
CLIENT001	No	No	Upgrade hardware and software.	Current operating system is Windows NT 4.0. Old hardware not compatible with Windows XP or Windows Vista.	$??	Isolated domain
SERVER002	Yes	No	Join trusted domain, upgrade from Windows NT 4.0 to Windows Server 2008	No antivirus software present.	$??	Encryption
SENSITIVE001	Yes	Yes	Not required.	Running Windows Server 2008. Ready for inclusion.	$0	Isolated server (in zone by itself)
PRINTSVR1	Yes	Yes	Not required.	Running Windows Server 2003. Ready for inclusion.	$0	Boundary

Next: Planning Group Policy Deployment for Your Isolation Zones

Planning Group Policy Deployment for Your Isolation Zones

After you have decided on the best logical design of your isolation environment for the network and computer security requirements, you can start the implementation plan.

You have a list of isolation zones with the security requirements of each. For implementation, you must plan the groups that will hold the computer accounts in each zone, the network access groups that will be used to determine who can access an isolated server, and the GPOs with the connection security and firewall rules to apply to corresponding groups. Finally you must determine how you will ensure that the policies will only apply to the correct computers within each group.

- Planning Isolation Groups for the Zones
- Planning Network Access Groups

- Planning the GPOs
- Planning GPO Deployment

Planning Isolation Groups for the Zones

Isolation groups in Active Directory are how you implement the various domain and server isolation zones. A computer is assigned to a zone by adding its computer account to the group which represents that zone.

Caution

> Do not add computers to your groups yet. If a computer is in a group when the GPO is activated then that GPO is applied to the computer. If the GPO is one that requires authentication, and the other computers have not yet received their GPOs, the computer that uses the new GPO might not be able to communicate with the others.

Universal groups are the best option to use for GPO assignment because they apply to the whole forest and reduce the number of groups that must be managed. However, if universal groups are unavailable, you can use domain global groups instead.

The following table lists typical groups that can be used to manage the domain isolation zones discussed in the Woodgrove Bank example this guide:

Group name	Description
CG_DOMISO_No_IPsec	A universal group of computer accounts that do not participate in the IPsec environment. Typically consists of infrastructure computer accounts that will also be included in exemption lists. This group is used in security group filters to ensure that GPOs with IPsec rules are not applied to group members.
CG_DOMISO_IsolatedDomain	A universal group of computer accounts that contains the members of the isolated domain. During the early days of testing, this group might contain only a very small number of computers. During production, it might contain the built-in **Domain Computers** group to ensure that every computer in the domain participates. Members of this group receive the domain isolation GPO that requires authentication for inbound connections.
CG_DOMISO_Boundary	A universal group of computer accounts that contains the members of the boundary zone.

Group name	Description
	Members of this group receive a GPO that specifies that authentication is requested, but not required.
CG_DOMISO_Encryption	A universal group of computer accounts that contains the members of the encryption zone. Members of this group receive a GPO that specifies that both authentication and encryption are required for all inbound connections.
CG_SRVISO_*ServerRole*	A universal group of computer accounts that contains the members of the server isolation group. Members of this group receive the server isolation GPO that requires membership in a network access group in order to connect. There will be one group for each set of servers that have different user and computer restriction requirements.
CG_DOMISO_WINDOWS2000	A universal group of computer accounts for all computers in the organization that are running Windows 2000. Because computers that are running Windows 2000 cannot process WMI filters, you must use security group filtering to prevent these computers from applying GPOs for other versions of Windows.

Multiple GPOs may be delivered to each group. Which one actually becomes applied depends on the security group filters assigned to the GPOs in addition to the results of any WMI filtering assigned to the GPOs. Details of the GPO layout are discussed in the section Planning the GPOs.

If multiple GPOs are assigned to a group, and similar rules are applied, the rule that most specifically matches the network traffic is the one that is used by the computer. For example, if one IPsec rule says to request authentication for all IP traffic, and a second rule from a different GPO says to require authentication for IP traffic to and from a specific IP address, then the second rule takes precedence because it is more specific.

Next: Planning Network Access Groups

Planning Network Access Groups

A network access group (NAG) is used to identify users and computers that have permission to access an isolated server. The server is configured to use firewall rules that allow only network connections that are authenticated as originating from a computer, and optionally a user, whose accounts are members of its NAG. A member of the isolated domain can belong to as many NAGs as required.

Minimize the number of NAGs to limit the complexity of the solution. You need one NAG for each server isolation group to restrict the computers that are granted access, and one additional NAG when you want access to the server isolation group to be restricted to only authorized users.

The NAGs that you create and populate become active by referencing them in the **Users and Computers** tab of the firewall rules in the GPO assigned to the isolated servers. The GPO must also contain connection security rules that require authentication to supply the credentials checked for NAG membership.

For the Woodgrove Bank scenario, access to the computers running SQL Server that support the WGBank application are restricted to the WGBank front-end servers and to approved administrative users logged on to specific authorized administrative computers. They are also only accessed by the approved admin users and the service account that is used to the run the WGBank front end service.

NAG Name	NAG Member Users, Computers, or Groups	Description
CG_NAG_*ServerRole*_Users	Svr1AdminA Svr1AdminB Group_AppUsers AppSvcAccount	This group is for all users who are authorized to make inbound IPsec connections to the isolated servers in this zone.
CG_NAG_*ServerRole*_Computers	Desktop1 Desktop2 AdminDT1 AppAdminDT1	This group contains all computers that are authorized to make inbound IPsec connections to the isolated servers in this zone.

Note

Membership in a NAG does not control the level of IPsec traffic protection. The IKE negotiation is only aware of whether the computer or user passed or failed the Kerberos V5 authentication process. The connection security rules in the applied GPO control the security methods that are used for protecting traffic and are independent of the identity being authenticated by Kerberos V5.

Next: Planning the GPOs

Planning the GPOs

When you plan the GPOs for your different isolation zones, you must complete the layout of the required zones and their mappings to the groups that link the computers to the zones.

General considerations

A few things to consider as you plan the GPOs:

- Do not allow a computer to be a member of more than one isolation zone. A computer in more than one zone receives multiple and possibly contradictory GPOs. This can result in unexpected, and difficult to troubleshoot behavior.

The examples in this guide show GPOs that are designed to prevent the requirement to belong to multiple zones.

- You must know the mix of computers that will be part of any specific zone. If the zone contains computers running Windows 2000, Windows XP and Windows Server 2003 as well as computers running Windows Vista and Windows Server 2008 then you must design multiple GPOs, one for each set of operating systems, with the appropriate IPsec policies, and including WMI filters to apply each GPO to the correct computers.

The Planning GPO Deployment section discusses how to ensure that each operating system version receives the correct GPO.

- Ensure that the IPsec algorithms you specify in your GPOs are compatible across all the versions of Windows. For example, if you have any computers running Windows 2000, then you must ensure that all computers include the main mode Diffie-Hellman Group 2 key exchange algorithm, because Windows 2000 cannot use more the advanced Diffie-Hellman groups. The same principle applies to the data integrity and encryption algorithms. We recommend that you include the more advanced algorithms when you have the option of selecting several in an ordered list. The computers will negotiate down from the top of their lists, selecting one that is configured on both computers. So a computer that is running Windows Vista that is connected to a server that is running Windows Server 2008 can communicate by using a much more secure algorithm, while computers running Windows 2000 or Windows XP connect to the same server by using a less secure, but compatible algorithm.
- The primary difference in your domain isolation GPOs is whether the rules request or require authentication.

Caution

It is **critical** that you begin with all your GPOs set to request authentication instead of requiring it. Since the GPOs are delivered to the computers over time, applying a require policy to one computer breaks its ability to communicate with another computer that has not yet received its policy. Using request mode at the beginning enables computers to continue communicating by using plaintext connections if required. After you confirm that your computers are using IPsec where expected, you can schedule a conversion of the rules in the GPOs from requesting to requiring authentication, as required by each zone.

- Windows Firewall with Advanced Security in Windows Vista and Windows Server 2008 only support one network location profile at a time. If you add a second network adapter that is connected to a different network, or not connected at all, you could unintentionally change the profile that is currently active on the computer. If your GPO specifies different firewall and connection security rules based on the current network location profile, the behavior of how the computer handles network traffic will change accordingly. We recommend for stationary computers, such as desktops and servers, that you assign any rule for the computer to all profiles. Apply GPOs that change rules per network location to computers that must move between networks, such as your portable computers. Consider creating a separate domain isolation GPO for your servers that uses the same settings as the GPO for the clients, except that the server GPO specifies the same rules for all network location profiles. For more information, see Network Location Types at http://go.microsoft.com/fwlink/?linkid=110826.
- Windows Server 2003 and Windows XP support only two network location profiles: domain and standard. The standard profile supported in those earlier versions of Windows is now split between the public and private profiles supported in Windows Vista and Windows Server 2008. If you apply a GPO with IPsec rules configured for the earlier versions of Windows to a computer that is running Windows Vista and Windows Server 2008, the rules for the standard profile are applied to only the private profile.

After considering these issues, document each GPO that you require, and the details about the connection security and firewall rules that it needs.

Woodgrove Bank example GPOs

The Woodgrove Bank example uses the following set of GPOs to support its domain isolation requirements. This section only discusses the rules and settings for server and domain isolation. GPO settings that affect which computers receive the GPO, such as security group filtering and WMI filtering, are discussed in the Planning GPO Deployment section.

In this section you can find information about the following:

- Firewall GPOs
- Isolated Domain GPOs
- Boundary Zone GPOs
- Encryption Zone GPOs
- Server Isolation GPOs

Firewall GPOs

All the computers on Woodgrove Bank's network that run Windows are part of the isolated domain, except domain controllers. To configure firewall rules, the two GPOs described in this section are linked to the domain container in the Active Directory OU hierarchy, and then filtered by using security group filters and WMI filters.

The GPOs created for the example Woodgrove Bank scenario include the following:

- GPO_DOMISO_Firewall_2008_Vista
- GPO_DOMISO_Firewall_2003_XP

GPO_DOMISO_Firewall_2008_Vista

This GPO is authored by using the Windows Firewall with Advanced Security interface in the Group Policy editing tools. The User Configuration section of the GPO is disabled. It is intended to only apply to computers that are running either Windows Server 2008 or Windows Vista.

Firewall settings

This GPO provides the following settings:

- Unless otherwise stated, the firewall rules and settings described here are applied to all profiles.
- The firewall is enabled, with inbound, unsolicited connections blocked and outbound connections allowed.
- Under the domain profile, the settings **Display notifications to the user**, **Apply local firewall rules**, and **Apply local connection security rules** are all set to **No**. These settings are applied only to the domain profile because the computers can only receive an exception rule for a required program from a GPO if they are connected to the domain. Under the public and private profiles, those settings are all set to **Yes**.

Note

Enforcing these settings requires that you define any firewall exceptions for programs, because the user cannot manually permit a new program. You must deploy the exception rules by adding them to this GPO. We recommend that you do not enable these settings until you have tested all your applications and have tested the resulting rules in a test lab and then on pilot computers.

Firewall rules

This GPO provides the following rules:

- Built-in firewall rule groups are configured to support typically required network operation. The following rule groups are set to **Allow the connection**:
  - Core Networking
  - File and Printer Sharing
  - Network Discovery
  - Remote Administration
  - Remote Desktop
  - Remote Event Log Management
  - Remote Scheduled Tasks Management
  - Remote Service Management
  - Remote Volume Management
  - Windows Firewall Remote Management
  - Windows Management Instrumentation (WMI)

    - Windows Remote Management

- A firewall exception rule to allow required network traffic for the WGBank dashboard program. This inbound rule allows network traffic for the program Dashboard.exe in the %ProgramFiles%\WGBank folder. The rule is also filtered to only allow traffic on port 1551. This rule is applied only to the domain profile.

Next: GPO_DOMISO_Firewall_2003_XP

GPO_DOMISO_Firewall_2003_XP

This GPO is authored by using the Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall section in the Group Policy editing tools. The User Configuration section of the GPO is disabled. It is intended to only apply to server computers that are running either Windows Server 2003 or Windows XP.

This GPO provides the following settings and rules:

- Most of the Windows Firewall settings described in this section are applied to both the domain and standard profiles. However, settings that prevent users from adding their own rules are enabled on the standard profile, but disabled on the domain profile. That ability is typically required when the user is not on the organization's network.
- The firewall is enabled and configured by modifying the settings shown in the following table.

Setting	Domain Profile	Standard Profile
Allow local program exceptions	**Disabled**	**Not configured**
Protect all network connections	**Enabled**	**Enabled**
Do not allow exceptions	**Disabled**	**Disabled**
Allow inbound file and printer sharing exception	**Enabled**, with address set to **192.168.0.0/16**	**Not configured**
Allow ICMP exceptions	**Enabled**, all check boxes selected	**Not configured**
Prohibit notifications	**Enabled**	**Not configured**
Allow local port exceptions	**Disabled**	**Not configured**
Allow inbound remote administration exception	**Enabled**, with address set to **192.168.0.0/16**	**Not configured**
Allow inbound Remote Desktop exceptions	**Enabled**, with address set to **192.168.0.0/16**	**Not configured**
Allow inbound UPnP framework exceptions	**Enabled**, with address set to **192.168.0.0/16**	**Not configured**

Note

By setting **Allow local program exceptions** and **Allow local port exceptions** to **Disable**, and by setting **Prohibit notifications** to **Enable**, you block users from manually allowing new programs. Therefore, you must define any required firewall exception rules for programs by adding them to this GPO. We recommend that you do not enable these settings until you have tested all your applications, created the required rules, and tested the resulting rules in a test lab and then on a set of pilot computers.

- An inbound program exception to allow traffic for the WGBank Dashboard program is assigned to the domain profile only, with the following text added:

%ProgramFiles%\WGBank\Dashboard.exe:192.168.0.0\16:Enabled:WGBank Dashboard

Next: Isolated Domain GPOs

Isolated Domain GPOs

All of the computers in the isolated domain are added to the group CG_DOMISO_IsolatedDomain. You must create multiple GPOs to align with this group, one for each Windows operating system that must have different rules or settings to implement the basic isolated domain functionality that you have in your isolated domain. This group is granted Read and Apply Group Policy permissions on all the GPOs described in this section.

Each GPO has a security group filter that prevents the GPO from applying to members of the group GP_DOMISO_No_IPsec. A WMI filter is attached to each GPO to ensure that the GPO is applied to only the specified version of Windows. Each GPO for versions of Windows other than Windows 2000 Server also has a security group filter that denies Read and Apply Group Policy permission to computers that run Windows 2000 Server. Likewise, the GPO for Windows 2000 Server has a WMI filter that enables the GPO to apply only to computers that are running Windows 2000 Server. For more information, see the Planning GPO Deployment section.

The GPOs created for the Woodgrove Bank isolated domain include the following:

- GPO_DOMISO_IsolatedDomain_Clients_WinVista
- GPO_DOMISO_IsolatedDomain_Servers_WS2008
- GPO_DOMISO_IsolatedDomain_Clients_WinXP
- GPO_DOMISO_IsolatedDomain_Servers_WS2003
- GPO_DOMISO_IsolatedDomain_Servers_Win2000

GPO_DOMISO_IsolatedDomain_Clients_WinVista

This GPO is authored by using the Windows Firewall with Advanced Security interface in the Group Policy editing tools. The User Configuration section of the GPO is disabled. It is intended to only apply to client computers that are running Windows Vista.

Because client computers can sometimes be portable, the settings and rules for this GPO are applied to only the domain profile.

General settings

This GPO provides the following settings:

- No firewall settings are included in this GPO. Woodgrove Bank created separate GPOs for firewall settings (see the Firewall GPOs section) in order to share them with all clients in all isolation zones with minimum redundancy.
- The ICMP protocol is exempted from authentication requirements to support easier network troubleshooting.
- Diffie-Hellman Group 2 is specified as the key exchange algorithm. This is the strongest algorithm available that is supported by all the operating systems that are being used at Woodgrove Bank. After Woodgrove Bank has completed the upgrade to versions of Windows that support stronger algorithms, such as Windows Vista or Windows Server 2008, they can remove the weaker key exchange algorithms, and use only the stronger ones.
- The main mode security method combinations in the order shown in the following table.

Integrity	Encryption
Secure Hash Algorithm (SHA-1)	Advanced Encryption Standard (AES-128)
SHA-1	3DES

- The following quick mode security data integrity algorithms combinations in the order shown in the following table.

Protocol	Integrity	Key Lifetime (minutes/KB)
ESP	SHA-1	60/100,000

- The quick mode security data integrity and encryption algorithm combinations in the order shown in the following table.

Protocol	Integrity	Encryption	Key Lifetime (minutes/KB)
ESP	SHA-1	AES-128	60/100,000
ESP	SHA-1	3DES	60/100,000

Note

Do not use the MD5 and DES algorithms in your GPOs. They are included only for compatibility with previous versions of Windows.

Connection Security Rules

This GPO provides the following rules:

- A connection security rule named **Isolated Domain Rule** with the following settings:
  - From **Any IP address** to **Any IP address**.
  - **Require inbound and request outbound** authentication requirements.

  Important

  On this, and all other GPOs that require authentication, Woodgrove Bank first chose to only request authentication. After confirming that the computers were successfully communicating by using IPsec, they switched the GPOs to require authentication.

  - For **First authentication methods**, select **Computer Kerberos v5** as the primary method. Add certificate-based authentication from **DC=com,DC=woodgrovebank,CN=CorporateCertServer** for computers that cannot run Windows or cannot join the domain, but must still participate in the isolated domain.
  - For **Second authentication**, select **User Kerberos v5**, and then select the **Second authentication is optional** check box.
- A connection security rule to exempt computers that are in the exemption list from the requirement to authenticate:
  - The IP addresses of all computers on the exemption list must be added individually under **Endpoint 2**.
  - Authentication mode is set to **Do not authenticate**.

Next: GPO_DOMISO_IsolatedDomain_Servers_WS2008

GPO_DOMISO_IsolatedDomain_Servers_WS2008

This GPO is authored by using the Windows Firewall with Advanced Security interface in the Group Policy editing tools. The User Configuration section of the GPO is disabled. It is intended to only apply to server computers that are running Windows Server 2008.

Since so many of the settings and rules for this GPO are common to those in the GPO for Windows Vista, you can save time by exporting the Windows Firewall with Advanced Security piece of the GPO for Windows Vista, and importing it to the GPO for Windows Server 2008. After the import, change only the items specified here:

- This GPO applies all its settings to all profiles: Domain, private, and public. Because a server is not expected to be mobile and changing networks, configuring the GPO in this manner prevents a network failure or addition of a new network adapter from unintentionally switching the computer to the Public profile with a different set of rules.

Important

Windows Vista and Windows Server 2008 support only one network location profile at a time. The profile for the least secure network type is applied to the computer. If you attach a network adapter to a computer that is not physically connected to a network, the public network location type is associated with the network adapter and applied to the computer.

Next: GPO_DOMISO_IsolatedDomain_Clients_WinXP

GPO_DOMISO_IsolatedDomain_Clients_WinXP

This GPO is authored by using the Computer Configuration\Windows Settings\Security Settings\IP Security Policies section in the GPO editing tools. The User Configuration section of the GPO is disabled. It is intended to only apply to server computers that are running Windows XP.

This GPO provides the following settings and rules:

IPsec rules

The GPO is configured to use the following IPsec elements:

IPsec filter lists

The GPO is configured to use the IP filter lists shown in the following table.

Name	Mirrored	Source <->Dest	Ports	Protocols
All IP Traffic	Yes	Any <-> Any	Any <-> Any	Any
ICMP Traffic	Yes	Any <-> Any	Any <-> Any	ICMP
Exemption List	Yes	Any <-> IP address list of all exempted hosts	Any <-> Any	Any

Note

You must set the source and destination addresses as shown in the previous table to ensure that Windows applies the filters correctly from most specific to most general.

IPsec filter actions

The GPO is configured to use the IPsec filter actions shown in the following table.

Name	Method	Algorithms AH|ESP:{integrity/encryption}	Key lifetime (KB/seconds)
Request Security	Negotiate Selected Selected	ESP:SHA1/none ESP:SHA1/3DES	100,000/3600
Allow Traffic	Permit Not applicable Not applicable	n/a	Not applicable
Require Security	Negotiate Cleared Selected	ESP:SHA1/none ESP:SHA1/3DES	100,000/3600

The Method column in the previous table includes of the following three settings in the following order:

- **Permit** / **Block** / **Negotiate security** options
- **Accept unsecured communication, but always respond using IPsec** check box. This is the inbound fallback-to-clear option.
- **Allow fallback to unsecured communication if a secure connection cannot be established** check box. This is the outbound fallback-to-clear option.

IPsec policies

The GPO is configured to use an IPsec policy named "Isolated Domain" that contains the rules shown in the following table. The rules are composed of the filter lists and filter actions that were configured earlier in this topic.

IP Filter list	Filter action	Authentication
All IP traffic	Require Security (see Caution below)	Kerberos V5 Certificate from internal CA
ICMP traffic	Allow Traffic	Not applicable
Exemption List	Allow Traffic	Not applicable

Caution

When the IPsec policy is first deployed, we strongly recommended that you first set the filter action to request security so that if any computers fail to receive the IPsec policy they can continue to communicate. After you confirm that all the computers are successfully communicating by using IPsec, change the filter action to require security.

IPsec registry settings

The GPO is configured to use the following custom registry settings. They are shown in the Group Policy Management Console (GPMC) by creating and adding an .adm file. The sample file shown in the Appendix A: Sample GPO Template File for Settings Used in this Guide section was used by Woodgrove Bank.

The registry settings are:

- **IPsec Default Exemptions** - Value set to **2** to exempt RSVP, Kerberos V5, and ISAKMP traffic. This value is documented in Knowledge Base article 810207 at http://go.microsoft.com/fwlink/?linkid=110516.
- **Simplified IPsec Policy** - Value set to **0x14** to improve the fallback to clear behavior of computers that run Windows XP and Windows Server 2003. This value is documented in Knowledge Base article 914841 at http://go.microsoft.com/fwlink/?linkid=110514. For the setting to work, all servers must have this update from the Knowledge Base article installed.

Neither registry entry has any effect on computers that are running Windows 2000 Server, so that if you share a GPO with both computers that run Windows 2000 Server or Windows Server 2003it will not cause any problems.

Next: GPO_DOMISO_IsolatedDomain_Servers_WS2003

GPO_DOMISO_IsolatedDomain_Servers_WS2003

This GPO is authored by using the Windows Firewall and IP Security Policies sections in the GPO editing tools. The User Configuration section of the GPO is disabled. It is intended to only apply to server computers that are running Windows Server 2003.

Because so many of the settings and rules for this GPO are common to those in the GPO for Windows XP, you can save time by exporting the IP Security Policies part of the GPO for Windows XP, and importing it the policy for Windows Server 2003. The firewall part of the GPO must be recreated by hand. Alternatively, you can copy the whole GPO for Windows XP, paste it as a new GPO in the **Group Policy Objects** container, and then change only the following items here:

- The Woodgrove Bank GPO for Windows Server 2003 is currently identical to the GPO for Windows XP. However, a separate GPO is maintained so that if any differences are required in the future, they are easy to add to only the correct set of computers. The registry entry settings in the GPO for Windows XP must also be duplicated in this GPO.

Next: GPO_DOMISO_IsolatedDomain_Servers_Win2000

GPO_DOMISO_IsolatedDomain_Servers_Win2000

This GPO is authored by using the IP Security Policies sections in the GPO editing tools. Windows 2000 Server does not have a built-in firewall. Therefore this guide does not discuss creating firewall policies for that version of Windows.

The basic policy settings for Windows Server 2003 and Windows 2000 Server are identical. Therefore you can save time by copying the whole GPO for Windows Server 2003, paste it as a new GPO in the **Group Policy Objects** container, and then change only the items that must be different as discussed here:

- The Woodgrove Bank GPO for Windows 2000 Server is currently identical to the GPO for Windows Server 2003. However, a separate GPO is maintained so that if any differences are required in the future, they are easy to add to only the correct set of computers.
- The registry settings included by adding an .adm file to the GPO are ignored by computers running Windows 2000 Server.

Next: Boundary Zone GPOs

Boundary Zone GPOs

All the computers in the boundary zone are added to the group CG_DOMISO_Boundary. You must create multiple GPOs to align with this group, one for each operating system that you have in your boundary zone. This group is granted Read and Apply permissions in Group Policy on the GPOs described in this section.

Note

> If you are designing GPOs for only Windows Vista and Windows Server 2008, you can design your GPOs in nested groups. For example, you can make the boundary group a member of the isolated domain group, so that it receives the firewall and basic isolated domain settings through that nested membership, with only the changes supplied by the boundary zone GPO. However, computers that are running older versions of Windows can only support a single IPsec policy being active at a time. The policies for each GPO must be complete (and to a great extent redundant with each other), because you cannot layer them as you can in the newer versions of Windows. For simplicity, this guide describes the techniques used to create the independent, non-layered policies. We recommend that you create and periodically run a script that compares the memberships of the groups that must be mutually exclusive and reports any computers that are incorrectly assigned to more than one group.

This means that you create a GPO for a boundary group for a specific operating system by copying and pasting the corresponding GPO for the isolated domain, and then modifying the new copy to provide the behavior required in the boundary zone.

The boundary zone GPOs are only for server versions of Windows. Client computers are not expected to participate in the boundary zone. If the need for one occurs, either create a new GPO for that version of Windows, or expand the WMI filter attached to one of the existing boundary zone GPOs to make it apply to the client version of Windows.

In the Woodgrove Bank example, only the GPO settings for a Web service on Windows Server 2008 or Windows Server 2003 are discussed. The equivalent GPO for Windows 2000 is functionally identical to the one for Windows Server 2003, with the exception of firewall rules that are not supported on Windows 2000.

- GPO_DOMISO_Boundary_WS2008
- GPO_DOMISO_Boundary_WS2003

GPO_DOMISO_Boundary_WS2008

This GPO is authored by using the Windows Firewall with Advanced Security interface in the Group Policy editing tools. Woodgrove Bank began by copying and pasting the GPO for the Windows Server 2008 version of the isolated domain GPO, and then renamed the copy to reflect its new purpose.

This GPO supports the ability for computers that are not part of the isolated domain to access specific servers that must be available to those untrusted computers. It is intended to only apply to server computers that are running Windows Server 2008.

IPsec settings

The copied GPO includes and continues to use the IPsec settings that configure key exchange, main mode, and quick mode algorithms for the isolated domain when authentication can be used.

Connection security rules

Rename the **Isolated Domain Rule** to **Boundary Zone Rule**. Change the authentication mode to **Request inbound and request outbound**. In this mode, the computer uses authentication when it can, such as during communication with a member of the isolated domain. It also supports the "fall back to clear" ability of request mode when an untrusted computer that is not part of the isolated domain connects.

Firewall rules

Copy the firewall rules for the boundary zone from the GPO that contains the firewall rules for the isolated domain. Customize this copy, removing rules for services not needed on servers in this zone, and adding inbound rules to allow the network traffic for the services that are to be accessed by other computers. For example, Woodgrove Bank added a firewall rule to allow inbound network traffic to TCP port 80 for Web client requests.

Make sure that the GPO that contains firewall rules for the isolated domain does not also apply to the boundary zone to prevent overlapping, and possibly conflicting rules.

Next: GPO_DOMISO_Boundary_WS2003

GPO_DOMISO_Boundary_WS2003

This GPO is authored by using the Windows Firewall and IP Security Policies sections in the GPO editing tools. Woodgrove Bank began by copying and pasting the GPO for the Windows Server 2003 version of the isolated domain GPO, and renamed the copy to reflect its new purpose.

This GPO supports the ability for computers that are not part of the isolated domain to access specific servers that must be available to those untrusted computers. It is intended to only apply to server computers that are running Windows Server 2003.

In addition to the existing filter lists, filter actions, and registry settings, the following are added to support computers in the boundary zone.

IP filter actions

Create the following IP filter action:

- **Name:** Request In/Out
- **Security Methods: Negotiate security**, with the same security method that is used in the isolated domain GPO.
- Select the **Accept unsecured communication, but always respond using IPsec** check box (the inbound fall back to clear option).
- Select the **Allow fallback to unsecured communication if a secure connection can not be established** check box (the outbound fall back to clear option).

IPsec policies

The GPO is configured to use an IPsec policy named "Boundary Zone Policy" that contains the rules shown in the following table.

IP Filter list	Filter action	Authentication
All IP traffic	Request In/Out	• Computer-based Kerberos V5 • Certificate from internal CA
ICMP traffic	Allow Traffic	Not applicable
Exemption List	Allow Traffic	Not applicable

- The same key exchange, main mode, and quick mode algorithms as specified in the isolated domain GPO for Windows Server 2003 are used here.
- The same registry settings added to the Windows Server 2003 isolated domain GPO by using a custom .adm file are included here, using the same values.
- After creating the Boundary Zone Policy, assign it as the active policy in the GPO.

Firewall rules

Copy the firewall rules for the boundary zone from the GPO that contains the firewall rules for the isolated domain. Customize this copy, removing rules for services not needed on servers in this zone, and adding inbound rules to allow the network traffic for the services that are to be accessed by other computers. For example, Woodgrove Bank added a firewall rule to allow inbound network traffic to TCP port 80 for Web client requests.

Make sure that the GPO that contains firewall rules for the isolated domain does not also apply to the boundary zone to prevent overlapping, and possibly conflicting rules.

Next: Encryption Zone GPOs

Encryption Zone GPOs

Handle encryption zones in a similar manner to the boundary zones. A computer is added to an encryption zone by adding the computer account to the encryption zone group. Woodgrove Bank has a single service that must be protected, and the computers that are running that service are added to the group CG_DOMISO_Encryption. This group is granted Read and Apply Group Policy permissions in on the GPOs described in this section.

The GPOs are only for server versions of Windows. Client computers are not expected to participate in the encryption zone. If the need for one occurs, either create a new GPO for that version of Windows, or expand the WMI filter attached to one of the existing encryption zone GPOs to make it apply to the client version of Windows.

- GPO_DOMISO_Encryption_WS2008
- GPO_DOMISO_Encryption_WS2003

GPO_DOMISO_Encryption_WS2008

This GPO is authored by using the Windows Firewall with Advanced Security interface in the Group Policy editing tools. Woodgrove Bank began by copying and pasting the GPO for the Windows Server 2008 version of the isolated domain GPO, and then renamed the copy to reflect its new purpose.

This GPO supports the ability for servers that contain sensitive data to require encryption for all connection requests. It is intended to only apply to server computers that are running Windows Server 2008.

IPsec settings

The copied GPO includes and continues to use the IPsec settings that configure key exchange, main mode, and quick mode algorithms for the isolated domain The following changes are made to encryption zone copy of the GPO:

The encryption zone servers require all connections to be encrypted. To do this, change the IPsec default settings for the GPO to enable the setting **Require encryption for all connection security rules that use these settings**. This disables all integrity-only algorithm combinations.

Connection security rules

Rename the **Isolated Domain Rule** to **Encryption Zone Rule**. Leave the authentication mode setting on **Require inbound and request outbound**. In this mode, the computer forces authentication for all inbound network traffic, and uses it when it can on outbound traffic.

Firewall rules

Copy the firewall rules for the encryption zone from the GPO that contains the firewall rules for the isolated domain. Customize this copy, removing rules for services not needed on servers in this zone, and adding inbound rules to allow the network traffic for the services that are to be accessed by other computers. For example, Woodgrove Bank added a firewall rule to allow inbound network traffic to TCP port 1433 for SQL Server client requests.

Change the action for every inbound firewall rule from **Allow the connection** to **Allow only secure connections**, and then select **Require the connections to be encrypted**.

Make sure that the GPO that contains firewall rules for the isolated domain does not also apply to the boundary zone to prevent overlapping, and possibly conflicting rules.

Next: GPO_DOMISO_Encryption_WS2003

GPO_DOMISO_Encryption_WS2003

This GPO is authored by using the Windows Firewall and IP Security Policies sections in the GPO editing tools. Woodgrove Bank began by copying and pasting the GPO for the Windows Server 2003 version of the isolated domain GPO, and then renamed the copy to reflect its new purpose.

This GPO supports the ability for servers that contain sensitive data to require encryption for all incoming connection requests. It is intended to only apply to server computers that are running Windows Server 2003.

In addition to the existing filter lists, filter actions, and registry settings, the following are added to support computers in the encryption zone.

IP filter actions

Create the following IP filter action:

- **Name:** Encrypt Traffic
- **Security Methods: Negotiate security**, with a security method of **Integrity and encryption** (defaults to SHA1 and 3DES).
- Select the **Accept unsecured communication, but always respond using IPsec** check box (the inbound fall back to clear option).
- Select the **Allow fallback to unsecured communication if a secure connection can not be established** check box (the outbound fall back to clear option).

IPsec policies

The GPO is configured to use an IPsec policy named "Encryption Zone Policy" that contains the rules shown in the following table.

IP filter list	Filter action	Authentication
All IP traffic	Encrypt Traffic	Kerberos V5 Certificate from internal CA
ICMP traffic	Allow Traffic	Not applicable
Exemption List	Allow Traffic	Not applicable

- The same key exchange, main mode, and quick mode algorithms as specified in the isolated domain GPO for Windows Server 2003 are used here.
- The same registry settings added to the Windows Server 2003 isolated domain GPO by using a custom .adm file are included here, using the same values.
- After creating the Boundary Zone Policy, assign it as the active policy in the GPO.

Firewall rules

Copy the firewall rules for the encryption zone from the GPO that contains the firewall rules for the isolated domain. Customize this copy, removing rules for services not needed on servers in this zone, and adding inbound rules to allow the network traffic for the services that are to be accessed by other computers. For example, Woodgrove Bank added a firewall rule to allow inbound network traffic to TCP port 1433 for SQL Server client requests.

Make sure that the GPO that contains firewall rules for the isolated domain does not also apply to the boundary zone to prevent overlapping, and possibly conflicting rules.

Next: Server Isolation GPOs

Server Isolation GPOs

Each set of computers that have different users or computers accessing them require a separate server isolation zone. Each zone requires one GPO for each version of Windows running on computers in the zone. The Woodgrove Bank example has an isolation zone for their computers that run SQL Server. The server isolation zone is logically considered part of the encryption zone. Therefore, server isolation zone GPOs must also include rules for encrypting all isolated server traffic. Woodgrove Bank copied the encryption zone GPOs to serve as a starting point, and renamed them to reflect their new purpose.

All of the computer accounts for computers in the SQL Server server isolation zone are added to the group CG_SRVISO_WGBANK_SQL. This group is granted Read and Apply Group Policy permissions in on the GPOs described in this section. The GPOs are only for server versions of Windows. Client computers are not expected to be members of the server isolation zone, although they can access the servers in the zone by being a member of a network access group (NAG) for the zone.

GPO_SRVISO_WS2008

This GPO is identical to the GPO_DOMISO_Encryption_WS2008 GPO with the following changes:

- The firewall rule that enforces encryption is modified to include the NAGs on the **Users and Computers** tab of the rule. The NAGs granted permission include CG_NAG_SQL_Users and CG_NAG_SQL_Computers.

Important

Earlier versions of Windows support only computer-based authentication. If you specify that user authentication is mandatory, only users on computers that are running Windows Vista or Windows Server 2008 can connect.

GPO_SRVISO_WS2003

This GPO is authored by using the Windows Firewall and IP Security Policies sections in the GPO editing tools. The User Configuration section of the policy is disabled. It is intended to only apply to server computers that are running Windows Server 2003.

This GPO is identical to the GPO_DOMISO_Encryption_WS2003 GPO with the following changes:

- Under **User Rights Assignment**, add the NAGs for users and computers to the **Access this computer from the network** user right. You must also remove the

Everyone, Power Users, and Users group from the user right list. The NAGs granted permission include CG_NAG_SQL_Users and CG_NAG_SQL_Computers.

GPO_SRVISO_WS2000

We recommend that you do not use computers that are running Windows 2000 as isolated servers. If information on these servers is sensitive enough to merit the protections of server isolation, we recommend that you use a computer that is running a version of Windows with stronger security, such as Windows Server 2008.

However, if business requirements are such that a computer running Windows 2000 Server must be placed in the boundary zone, design the GPO as follows:

- The basic policy settings for Windows Server 2003 and Windows 2000 are identical. Therefore you can save time by copying the whole GPO for Windows Server 2003, pasting it as a new GPO in the **Group Policy Objects** container, and then changing only the items that must be different. In the Woodgrove Bank example, the settings are the same, and no differences must be accounted for.

We recommend that you create a separate GPO to support the ability to make operating system version specific changes, in case the need occurs.

Next: Planning GPO Deployment

Planning GPO Deployment

You can control which GPOs are applied to computers in Active Directory in a combination of three ways:

- **Active Directory organizational unit hierarchy**. This involves linking the GPO to a specific OU in the Active Directory OU hierarchy. All computers in the OU and its subordinate containers receive and apply the GPO.

Controlling GPO application through linking to OUs is typically used when you can organize the OU hierarchy according to your domain isolation zone requirements. GPOs can apply settings to computers based on their location within Active Directory. If a computer is moved from one OU to another, the policy linked to the second OU will eventually take effect when Group Policy detects the change during polling.

- **Security group filtering**. This involves linking the GPOs to the domain level (or other parent OU) in the OU hierarchy, and then selecting which computers receive the GPO by using permissions that only allow correct group members to apply the GPO.

The security group filters are attached to the GPOs themselves. A group is added to the security group filter of the GPO in Active Directory, and then assigned Read and Apply Group Policy permissions. Other groups can be explicitly denied Read and Apply Group Policy permissions. Only those computers whose group membership are granted Read and Apply Group Policy permissions without any explicit deny permissions can apply the GPO.

- **WMI filtering**. A WMI filter is a query that is run dynamically when the GPO is evaluated. If a computer is a member of the result set when the WMI filter query runs, the GPO is applied to the computer.

A WMI filter consists of one or more conditions that are evaluated against the local computer. You can check almost any characteristic of the computer, its operating system, and its installed programs. If all of the specified conditions are true for the computer, the GPO is applied; otherwise the GPO is ignored.

Important

Computers running Windows 2000 Server ignore WMI filtering and will apply the GPO even if the WMI filter is written to explicitly exclude Windows 2000 Server. Having computers that run Windows 2000 Server on the network is a common reason for combining both security group filtering and WMI filtering.

This guide uses a combination of security group filtering and WMI filtering to provide the most flexible options. If you follow this guidance, even though there might be five different GPOs linked to a specific group because of operating system version differences, only the correct GPO is applied.

General considerations

- Because Windows 2000 Server does not support WMI filters, you must add all the computers running Windows 2000 Server to a group such as CG_DOMISO_WINDOWS2000, and set a security group filter using that group on the GPOs for the other operating systems that prevents their application to the members of the Windows 2000 Server group. Set a WMI filter on the GPO for the computers running Windows 2000 Server that prevents it from being applied to later versions of Windows.
- Deploy your GPOs before you add any computer accounts to the groups that receive the GPOs. That way you can add your computers to the groups in a controlled manner. Be sure to add only a few test computers at first. Before adding many group members, examine the results on the test computers and verify that the configured firewall and connection security rules have the effect that you want. See the following sections for some suggestions on what to test before you continue.

Test your deployed groups and GPOs

After you have deployed your GPOs and added some test computers to the groups, confirm the following before you continue with more group members:

- Examine the GPOs that are both assigned to and filtered from the computer. Run the **gpresult** tool at a command prompt.
- Examine the rules deployed to the computer. Open the Windows Firewall with Advanced Security MMC snap-in, expand the **Monitoring** node, and then expand the **Firewall** and **Connection Security** nodes.
- Verify that communications are authenticated. Open the Windows Firewall with Advanced Security MMC snap-in, expand the **Monitoring** node, expand the **Security Associations** node, and then click **Main Mode**.
- Verify that communications are encrypted when the computers require it. Open the Windows Firewall with Advanced Security MMC snap-in, expand the **Monitoring** node,

expand the **Security Associations** node, and then select **Quick Mode**. Encrypted connections display a value other than **None** in the **ESP Confidentiality** column.

- Verify that your programs are unaffected. Run them and confirm that they still work as expected.

After you have confirmed that the GPOs have been correctly applied, and that the computers are now communicating by using IPsec network traffic in request mode, you can begin to add more computers to the group accounts, in manageable numbers at a time. Continue to monitor and confirm the correct application of the GPOs to the computers.

Do not enable require mode until deployment is complete

If you deploy a GPO that requires authentication to a computer before the other computers have a GPO deployed, communication between them might not be possible. Wait until you have all the zones and their GPOs deployed in request mode and confirm (as described in the previous section) that the computers are successfully communicating by using IPsec.

If there are problems with GPO deployment, or errors in configuration of one or more of the IPsec GPOs, computers can continue to operate, because request mode enables any computer to fall back to clear communications.

Only after you have added all of the computers to their zones, and you have confirmed that communications are working as expected, you can start changing the request mode rules to require mode rules where it is required in the zones. We recommend that you enable require mode in the zones one zone at a time, pausing to confirm that they are functioning properly before you continue. Turn the required mode setting on for the server isolation zones first, then the encryption zone, and then the isolated domain.

Do not change the boundary zone GPO, because it must stay in request mode for both inbound and outbound connections.

If you create other zones that require either inbound or outbound require mode, make the setting change in a manner that applies the setting in stages from the smaller groups of computers to the larger groups.

Example Woodgrove Bank deployment plans

Woodgrove Bank links all its GPOs to the domain level container in the Active Directory OU hierarchy. It then uses the following WMI filters and security group filters to control the application of the GPOs to the correct subset of computers. All of the GPOs have the User Configuration section disabled to improve performance.

GPO_DOMISO_Firewall_2008_Vista

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
  - `select * from Win32_OperatingSystem where Version like "6.0%"`
  - `select * from Win32_OperatingSystem where ProductType= "1" or ProductType= "3"`

Note

This excludes domain controllers (which report a ProductType value of 2). Do not include domain controllers in the isolated domain if there are computers running versions of Windows earlier than Windows Vista and Windows Server 2008.

- **Security filter**. This GPO grants Read and Apply Group Policy permissions in only to computers that are members of the group CG_DOMISO_IsolatedDomain. The GPO also explicitly denies Read and Apply Group Policy permissions to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

GPO_DOMISO_Firewall_2003_XP

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
    - `select * from Win32_OperatingSystem where Version like "5.2%" or Version like "5.1%"`
    - `select * from Win32_OperatingSystem where ProductType= "1" or ProductType= "3"`

Note

This excludes domain controllers (which report a ProductType value of 2). Do not include domain controllers in the isolated domain if there are computers that are running versions of Windows earlier than Windows Vista and Windows Server 2008.

- **Security filter**. This GPO grants Read and Apply Group Policy permissions only to computers that are members of the group CG_DOMISO_IsolatedDomain. The GPO also explicitly denies Read and Apply Group Policy permissions to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

GPO_DOMISO_IsolatedDomain_Clients_WinVista

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
    - `select * from Win32_OperatingSystem where Version like "6.0%"`
    - `select * from Win32_OperatingSystem where ProductType = "1"`
- **Security filter**. This GPO grants Read and Apply Group Policy permissions only to computers that are members of the group CG_DOMISO_IsolatedDomain. The GPO also explicitly denies Read and Apply Group Policy permissions to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

GPO_DOMISO_IsolatedDomain_Servers_WS2008

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
    - `select * from Win32_OperatingSystem where Version like "6.0%"`
    - `select * from Win32_OperatingSystem where ProductType = "3"`

Note

This excludes domain controllers (which report a ProductType value of 2). Do not include domain controllers in the isolated domain if there are computers that are running versions of Windows earlier than Windows Vista and Windows Server 2008.

- **Security filter**. This GPO grants Read and Apply Group Policy permissions only to computers that are members of the group CG_DOMISO_IsolatedDomain. The GPO also explicitly denies Read and Apply Group Policy permissions to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

GPO_DOMISO_IsolatedDomain_Clients_WinXP

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
    - `select * from Win32_OperatingSystem where Version like "5.1%"`
    - `select * from Win32_OperatingSystem where ProductType = "1"`
- **Security filter**. This GPO grants Read and Apply Group Policy permissions only to computers that are members of the group CG_DOMISO_IsolatedDomain. The GPO also explicitly denies Read and Apply Group Policy permissions to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

GPO_DOMISO_IsolatedDomain_Servers_WS2003

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
    - `select * from Win32_OperatingSystem where Version like "5.2%"`
    - `select * from Win32_OperatingSystem where ProductType = "3"`

Note

This excludes domain controllers (which report a ProductType value of 2). Do not include domain controllers in the isolated domain if there are computers that are running versions of Windows earlier than Windows Vista and Windows Server 2008.

- **Security filter**. This GPO grants Read and Apply Group Policy permissions only to computers that are members of the group CG_DOMISO_IsolatedDomain. The GPO also explicitly denies Read and Apply Group Policy permissions to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

GPO_DOMISO_IsolatedDomain_Servers_Win2000

- **WMI filter**. The WMI filter attached to this GPO allows it to apply to only computers that report an operating system version of 5.0. This is to prevent the GPO from applying to computers that are running later versions of Windows. Because computers running Windows 2000 Server cannot process WMI filters, all GPOs apply unless the GPO also has a security group filter that prevents the computer from reading or apply the GPO.
- **Security filter**. This GPO grants Read and Apply Group Policy permissions only to computers that are members of the group CG_DOMISO_WINDOWS2000.

GPO_DOMISO_Boundary_WS2008

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
  - `select * from Win32_OperatingSystem where Version like "6.0%"`
  - `select * from Win32_OperatingSystem where ProductType = "3"`

Note

This excludes domain controllers (which report a ProductType value of 2). Do not include domain controllers in the isolated domain if there are computers that are running versions of Windows earlier than Windows Vista and Windows Server 2008.

- **Security filter**. This GPO grants Read and Apply Group Policy permissions only to computers that are members of the group CG_DOMISO_Boundary. The GPO also explicitly denies Read and Apply Group Policy permissions to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

GPO_DOMISO_Boundary_WS2003

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
  - `select * from Win32_OperatingSystem where Version like "5.2%"`
  - `select * from Win32_OperatingSystem where ProductType = "3"`

Note

This excludes domain controllers (which report a ProductType value of 2). Do not include domain controllers in the isolated domain if there are computers that are running versions of Windows earlier than Windows Vista and Windows Server 2008.

- **Security filter**. This GPO grants Read and Apply permissions in Group Policy only to computers that are members of the group CG_DOMISO_Boundary. The GPO also explicitly denies Read and Apply permissions in Group Policy to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

GPO_DOMISO_Encryption_WS2008

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
  - `select * from Win32_OperatingSystem where Version like "6.0%"`
  - `select * from Win32_OperatingSystem where ProductType = "3"`

Note

This excludes domain controllers (which report a ProductType value of 2). Do not include domain controllers in the isolated domain if there are computers that are running versions of Windows earlier than Windows Vista and Windows Server 2008.

- **Security filter**. This GPO grants Read and Apply permissions in Group Policy only to computers that are members of the group CG_DOMISO_Boundary. The GPO also explicitly denies Read and Apply permissions in Group Policy to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

GPO_DOMISO_Encryption_WS2003

- **WMI filter**. The WMI filter allows this GPO to apply only to computers that match the following WMI queries:
    - select * from Win32_OperatingSystem where Version like "5.2%"
    - select * from Win32_OperatingSystem where ProductType = "3"

Note

This excludes domain controllers (which report a ProductType value of 2). Do not include domain controllers in the isolated domain if there are computers that are running versions of Windows earlier than Windows Vista and Windows Server 2008.

- **Security filter**. This GPO grants Read and Apply permissions in Group Policy only to computers that are members of the group CG_DOMISO_Boundary. The GPO also explicitly denies Read and Apply permissions in Group Policy to members of the group CG_DOMISO_Windows2000, and to the group CG_DOMISO_NO_IPSEC.

Next: Appendix A: Sample GPO Template File for Settings Used in this Guide

Appendix A: Sample GPO Template File for Settings Used in this Guide

The following sample illustrates how to build an .adm file that can be loaded into Group Policy Management Console to enable setting registry key values by using Group Policy.

To use this in a test environment, copy and paste the following sample text into Notepad, and save the file with an .adm file name extension on the computer that you use to manage your GPOs, and then complete the following procedure.

To load a custom .adm file into your GPO

1. Open the GPO that you want to modify in Group Policy Management Console.
2. Under **Computer Configuration**, right-click **Administrative Templates**, and then click **Add/Remove Templates**.
3. In the **Add/Remove Templates** dialog box, click **Add**.
4. In the **Policy Templates** dialog box, browse to the folder that contains your .adm file, select it, and then click **Open**.
5. If you are only adding the one .adm file, click **Close**. Otherwise, repeat steps 3 and 4.
6. Expand the **Administrative Templates** node, and then expand the **Classic Administrative Templates (ADM)** node.
7. Browse this node to find your custom settings.

Sample code for an .adm file

```
CLASS MACHINE

CATEGORY !!CATNAME
```

```
    POLICY !!POL1NAME
        KEYNAME "SYSTEM\CurrentControlSet\Services\IPSEC"
        EXPLAIN !!POL1EXPLAIN
        PART !!DROPDOWNLIST1NAME DROPDOWNLIST REQUIRED
            VALUENAME "NoDefaultExempt"
            ITEMLIST
                NAME !!ITEMNAME10 VALUE NUMERIC 0
                NAME !!ITEMNAME11 VALUE NUMERIC 1
                NAME !!ITEMNAME12 VALUE NUMERIC 2 Default
                NAME !!ITEMNAME13 VALUE NUMERIC 3
            END ITEMLIST
        END PART
    END POLICY
    POLICY !!POL2NAME
        KEYNAME "SYSTEM\CurrentControlSet\Services\PolicyAgent\Oakley"
        EXPLAIN !!POL2EXPLAIN
        PART !!DROPDOWNLIST2NAME DROPDOWNLIST REQUIRED
            VALUENAME "IKEFlags"
            ITEMLIST
                NAME !!ITEMNAME20 VALUE NUMERIC 0
                NAME !!ITEMNAME21 VALUE NUMERIC 4
                NAME !!ITEMNAME22 VALUE NUMERIC 16
                NAME !!ITEMNAME23 VALUE NUMERIC 20 Default
            END ITEMLIST
        END PART
    END POLICY
END CATEGORY
[strings]
CATNAME="Additional IPsec Settings for Server and Domain Isolation"
POL1NAME="IPsec Default Exemptions"
POL1EXPLAIN="This setting specifies which protocols are exempt from IPsec protection. The settings are documented in Microsoft Knowledge Base article 810207 at http://support.microsoft.com/kb/810207."
DROPDOWNLIST1NAME="Select the protocols to be exempted from IPsec protection:"
ITEMNAME10="0: Multicast, broadcast, RSVP, Kerberos, ISAKMP"
```

```
ITEMNAME11="1: Multicast, broadcast, ISAKMP"
ITEMNAME12="2: RSVP, Kerberos, ISAKMP"
ITEMNAME13="3: ISAKMP"
POL2NAME="Simplified IPsec Policy"
POL2EXPLAIN="This setting specifies how Windows Server 2003 and Windows XP handle the
fallback-to-clear (FBTC) option. It requires the installation of a the update available
at Microsoft Knowledge Base Article 814841 at
http://support.microsoft.com/default.aspx/kb/914841."
DROPDOWNLIST2NAME="Select one of the following fall-back-to-clear (FBTC) options:"
ITEMNAME20="0x00: Original 3 second FBTC"
ITEMNAME21="0x04: Enables 500ms FBTC behavior"
ITEMNAME22="0x10: Improve FBTC in S&D Iso"
ITEMNAME23="0x14: Both 0x4 and 0x10 settings enabled (recommended)"
```

Next: Additional Resources

Additional Resources

For more information about the technologies discussed in this guide, see topics referenced in the following sections.

Windows Firewall with Advanced Security

- **Windows Firewall** (http://go.microsoft.com/fwlink/?linkid=95393)

  This TechNet page contains links to a variety of documents available for Windows Firewall, for Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

- **Windows Firewall with Advanced Security Content Roadmap** (http://go.microsoft.com/fwlink/?linkid=96525)

  This topic describes the documents currently available in the Windows Technical Library for Windows Firewall with Advanced Security in Windows Vista 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 TechNet page contains links to a variety of documents currently available for Internet Protocol security (IPsec), for Windows XP, Windows Server 2003, and the version available as connection security rules in Windows Firewall with Advanced Security on Windows Vista 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 SP1. 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 TechNet page contains links to documentation about the most common uses for IPsec: server isolation and domain isolation. Documentation is available for Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

Group Policy

Group Policy is a key method for implementing firewall and server and domain isolation designs.

For more information about Group Policy and related technologies, see:

- **Group Policy** (http://go.microsoft.com/fwlink/?linkid=93542)

This page contains links to the documents currently available for Group Policy, for both the version available in Windows XP and Windows Server 2003, and the version available in Windows Vista and Windows Server 2008.

- **WMI Filtering Using GPMC** (http://go.microsoft.com/fwlink/?linkid=93188)
- **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.

Active Directory Domain Services

In Windows Server 2008, organizations can use AD DS to manage users and resources, such as computers, printers, or applications, on a network. Server isolation and domain isolation also require AD DS to use the Kerberos V5 protocol for IPsec authentication.

For more information about AD DS and related technologies, see:

- **Active Directory Domain Services** (http://go.microsoft.com/fwlink/?linkid=102573)