

Module 6: Configuring Network Security by Using IPSec

Contents

Overview	1
Introduction to IPSec	2
Implementing IPSec	7
Configuring TCP/IP for Server Security	19
Troubleshooting Network Protocol Security	20
Lab A: Configuring TCP/IP for Secure Connections by Using IPSec	22
Review	28



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, BackOffice, FrontPage, IntelliMirror, NetShow, Outlook, PowerPoint, Visual Studio, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Simulations and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
45 Minutes

This module provides students with the knowledge and skills necessary to configure network security by using Internet Protocol Security (IPSec) in a Microsoft® Windows® 2000 network.

Lab:
45 Minutes

At the end of this module, students will be able to:

- Describe the use of IPSec in a network.
- Implement IPSec.
- Configure IPSec for server security.
- Troubleshoot network protocol security.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the Microsoft PowerPoint® file 2153a_06.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Read the *Step-by-Step Guide to Internet Protocol Security (IPSec)* at <http://www.microsoft.com/windows2000/library/technologies/security/default.asp>.
- Read the white paper *IP Security for Microsoft Windows 2000 Server*.
- Read the entire “Internet Protocol Security” section in the Windows 2000 Server Resource Kit.
- Read RFC 2401, *Security Architecture for the Internet Protocol*.
- Read RFC 2411, *IP Security Document Roadmap*.

Module Strategy

Use the following strategy to present this module:

- Introduction to IPSec

Introduce IPSec by discussing the need for security in both private and public networks. Briefly describe a few of the common types of network attacks. Use the slide to describe the components and processes associated with IPSec in a network. Give examples of business scenarios in which IPSec would be useful.

- Implementing IPSec

Explain that IPSec is enabled by using a policy configuration and emphasize that policies enable administrators to configure security settings automatically. Explain the use of IPSec in transport and tunnel modes, ensuring that students understand the difference between the two. Explain how IPSec security policies can be customized, and describe the components of rules. Briefly mention the options available for encryption, and refer students to the applicable white papers for more detail. Explain how to test IPSec policy assignments by using ping and IPSec Monitor.

- Configuring TCP/IP for Server Security

Explain the purpose of enabling IPSec for server security, and show students how to assign the Secure Server security policy.

- Troubleshooting Network Protocol Security

Explain the process for troubleshooting network protocol security and the methods that you can use to verify the IPSec policy.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Lab Setup

There are no lab setup requirements that affect replication or customization.

Lab Results

The following list describes the setup requirements for the lab in this module.

Setup Requirements

The lab in this module requires that student computers have a certificate installed that has been issued for use with IPSec. Student computers in each pair must trust the certification path of the Certificate Authority (CA) that issued the certificate. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete module 5, “Configuring Network Security by Using Public Key Infrastructure,” in course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.
- Perform the following steps manually. Refer to lab A, “Installing and Configuring Certificate Services” of module 5, “Configuring Network Security by Using Public Key Infrastructure,” in course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*, for detailed instructions.
 - On the instructor computer or on a student computer, create a stand-alone root CA.
 - On each student computer, add the CA as a trusted root CA.
 - On the student computer, request a certificate from the CA for use with IPSec by using a Web page.
 - Issue the certificate on the CA.
 - Install the certificate on the student computer.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about implementing IPSec to provide network security.

- Introduction to IPSec
- Implementing IPSec
- Configuring TCP/IP for Server Security
- Troubleshooting Network Protocol Security

*****ILLEGAL FOR NON-TRAINER USE*****

Because the loss of proprietary information can compromise an organization's success, an organization needs to have reliable network security for sensitive information, such as product data, financial reports, and marketing plans. Internet Protocol Security (IPSec) is a framework of open standards for ensuring secure, private communications over Internet Protocol (IP) networks by using cryptographic security services.

You can implement IPSec in a Microsoft® Windows® 2000 network to authenticate computers and encrypt data for transmission between hosts in a network, intranet, or extranet, including workstation-to-server and server-to-server communications.

At the end of this module, you will be able to:

- Describe the use of IPSec in a network.
- Implement IPSec.
- Configure IPSec for server security.
- Troubleshoot network protocol security.

◆ Introduction to IPSec

Topic Objective

To introduce the topics related to IPSec.

Lead-in

Without security, both public and private networks are susceptible to unauthorized monitoring and access.

- Identifying Security Issues with Networks
- Examining the Role of IPSec in a Network

*****ILLEGAL FOR NON-TRAINER USE*****

Without security, both public and private networks are susceptible to unauthorized monitoring and access. Internal attacks might be a result of minimal or nonexistent intranet security, whereas risks from outside the private network stem from connections to the Internet and extranets. IPSec protects private data in a public environment by providing a strong, cryptography-based defense against network attacks.

Note IPSec is an Internet Engineering Task Force (IETF) proposal and is not yet an IETF standard. For more information about IPSec, see RFC 2411 and RFC 2401 under **Additional Reading** on the Student Materials compact disc.

For a more extensive list of applicable RFCs, see the “Internet Protocol Security” section of the Windows 2000 Server Resource Kit.

Identifying Security Issues with Networks

Topic Objective

To identify common types of network attacks.

Lead-in

Security attacks can be passive or active.

Common Types of Network Attacks

- Network monitoring
- Data modification
- Passwords
- Address spoofing
- Application-layer
- Man-in-the-middle
- Denial-of-service

*****ILLEGAL FOR NON-TRAINER USE*****

Whether over the Internet, an intranet, or to and from branch-office or remote employees, sensitive information is constantly crossing the networks. The challenge for network administrators is to ensure that this data is:

- Safe from modification while in transit.
- Safe from interception, viewing, or copying.
- Safe from being accessed by unauthenticated parties.

You can implement IPSec to secure communications within an intranet and to create secure virtual private network (VPN) solutions across the Internet. IPSec can protect communication between workgroups, local area network (LAN) computers, domain clients and servers, branch offices that are physically remote, extranets, remote clients, and remote administration of computers.

Common Types of Network Attacks

Without security measures and controls in place, your data might be vulnerable to an attack. Some attacks are passive, meaning that an unknown outsider is monitoring your information; others are active, meaning that an assailant is altering information with the intent to corrupt or destroy the data or the network itself. Below is a partial list of the most common network attacks:

Explain that network-monitoring tools are often called "sniffers."

- *Network monitoring.* A network monitor is an application or device that can observe and read network packets. If the packets are not encrypted, a network-monitoring tool provides a full view of the data inside the packet. Such applications are useful for diagnostic purposes, but they can be misused to obtain unauthorized access to data. Microsoft Network Monitor is an example of a network-monitoring tool.
- *Data modification.* An attacker can modify a message in transit and send counterfeit data, which can prevent the receiver from receiving the correct information or can allow the attacker to obtain secure information.
- *Passwords.* An attacker can use a stolen password or key, or attempt to decipher the password if it is a simple password.
- *Address spoofing.* An attacker can use special programs to construct IP packets that appear to originate from valid addresses inside the trusted network.
- *Application-layer.* This attack targets application servers by exploiting weaknesses in server operating systems and applications.
- *Man-in-the-middle.* In this attack, someone between the two communicating computers actively monitors, captures, and controls the data transparently (for example, the attacker can reroute a data exchange).
- *Denial-of-service.* The goal of this attack is to prevent normal use of computers or network resources. For example, denial-of-service attacks may occur when e-mail accounts are flooded with more unsolicited messages than the system can handle, which can subsequently shut down the server.

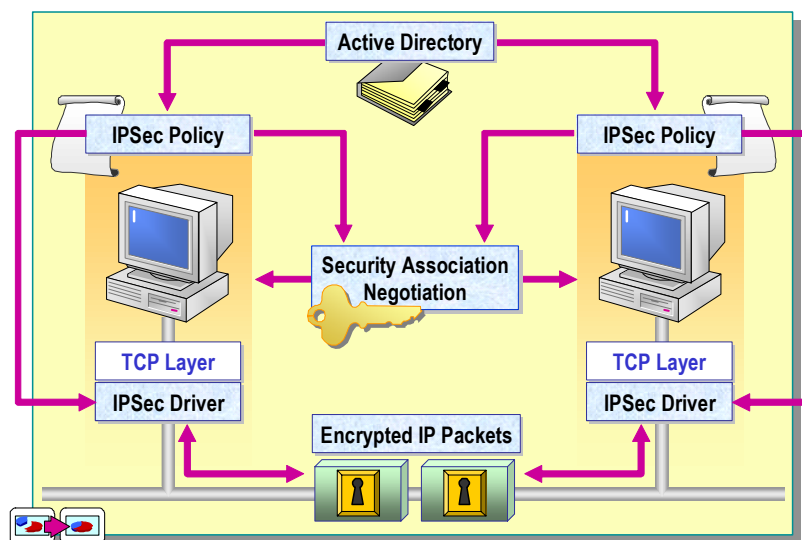
Examining the Role of IPSec in a Network

Topic Objective

To illustrate the IPSec components and processes in a network.

Lead-in

IPSec creates secure communication between clients, servers, and networks, without user intervention.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide for this topic includes animation. Click or press the SPACEBAR to advance the animation.

The primary goal of IPSec is to provide protection for IP packets. IPSec is based on an end-to-end security model, meaning that the sender and the receiver are the only hosts that must know about the IPSec protection. Each computer handles security at its own end under the assumption that the medium over which the communication takes place is not secure. Computers that only route data from source to destination are not required to support IPSec.

Enhanced Network Security

IPSec enhances network data security by:

- Mutually authenticating computers prior to data exchange.
- Establishing a security association between the two computers.
- Encrypting exchanged data.

IPSec uses standard IP packet formats when authenticating or encrypting data. Therefore, intermediary network devices, such as routers, do not have to handle IPSec packets differently from standard IP packets.

IPSec Policies

IPSec is implemented by using an IPSec *policy*. Policies are security settings, or *rules*, that define the level of security that you want, in addition to the addresses, protocols, Domain Name System (DNS) names, subnets, or connection types to which the security settings will apply. The IPSec *driver* matches every incoming and outgoing packet against the security settings defined in the active IPSec policy. You can apply IPSec policies to local computers, domain members, domains, or to multiple computers by using a Group Policy object in the Active Directory™ directory service.

Note Several vendors are working on implementing IPSec in other operating systems and network devices, such as routers. For more information about how Windows 2000 uses IPSec, see the white paper *IP Security for Microsoft Windows 2000 Server* under **Additional Reading** on the Student Materials compact disc and the *Step-by-Step Guide to Internet Protocol Security (IPSec)* at <http://www.microsoft.com/windows2000/library/technologies/security/default.asp>.

◆ Implementing IPSec

Topic Objective

To identify the topics related to implementing IPSec.

Lead-in

Windows 2000 provides policy-based administration to implement IPSec services.

- Enabling IPSec
- Configuring IPSec for Security Between Computers
- Configuring IPSec for Security Between Networks
- Customizing IPSec Policies
- Choosing an Encryption Scheme
- Testing an IPSec Policy Assignment
- Optimizing IPSec Performance

*****ILLEGAL FOR NON-TRAINER USE*****

Although stronger security methods based on cryptography have become necessary to fully protect communication, implementing these methods can greatly increase administrative overhead. Windows 2000 provides policy-based administration to implement IPSec services. Policies enable an administrator to configure security settings automatically. A network security administrator can configure IPSec policies to meet the security requirements of a user, group, domain, site, or enterprise. Windows 2000 provides an administrative interface, called IPSec Policy Management, to define IPSec policies for computers at the Active Directory level for any domain members or on the local computer for nondomain members.

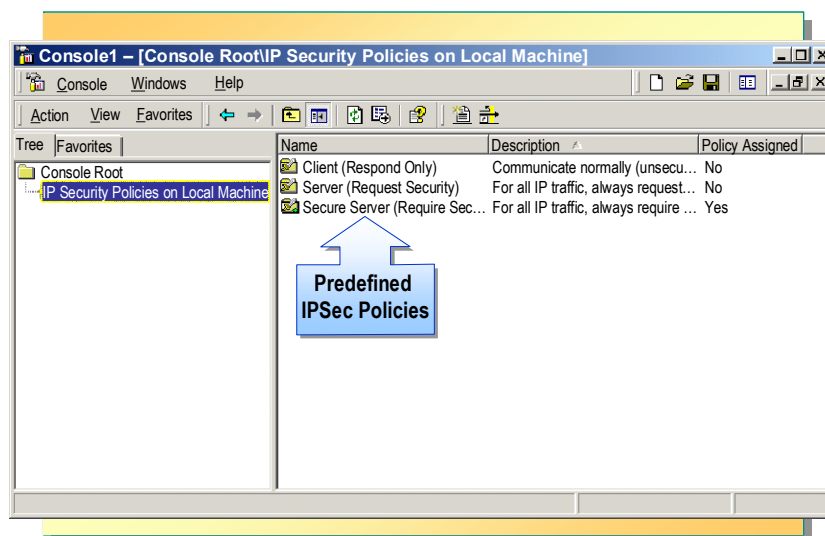
Enabling IPSec

Topic Objective

To illustrate the interface for configuring IPSec policies.

Lead-in

You manage IPSec policies through MMC, and you can define them in Active Directory, on the local computer, or on a remote computer.



*****ILLEGAL FOR NON-TRAINER USE*****

You control IPSec by using a policy configuration that you manage in IP Security Policy Management. You use IP Security Policy Management to manage IPSec policies centrally for Active Directory clients, locally for the computer on which you are running the console, or remotely for a computer or domain.

Note To configure IPSec policies for computers, you must have the appropriate administrator rights to Group Policy or be a member of the local system's Administrators group.

Managing IPSec Policies

You manage IPSec policies by adding the IP Security Policy Management snap-in to a Microsoft Management Console (MMC) console. After adding the IP Security Policy Management snap-in to a console, select the computer for which you want to manage IPSec policies:

To	Do this
Manage only the computer on which the console is running	Click Local Computer .
Manage IPSec policies for any domain members	Click Manage domain policy for this computer's domain .
Manage IPSec policies for a domain of which the computer that is running this console is not a member	Click Manage domain policy for another domain .
Manage a remote computer	Click Another computer .

You can then save the customized console so that it is available to you again at any time.

Using Predefined IPSec Policies

Windows 2000 provides a set of predefined IPSec policies. By default, all predefined policies are designed for computers that are members of a Windows 2000 domain. You can assign predefined policies without further action, or you can modify them, or use them as a template for defining custom policies.

Client (Respond Only)

Explain that rules that comprise the policies will be discussed next in the module.

This policy is for computers that do not require secure communications; for example, intranet clients that only use IPSec when requested by another computer. This policy enables the computer to respond appropriately to requests for secured communications. The policy contains a default response rule, which enables negotiation with computers requesting IPSec.

Server (Request Security)

This policy is for computers that require secure communications most of the time; for example, servers that transmit sensitive data. This policy enables the computer to accept unsecured traffic, but always attempts to secure additional communications by requesting security from the original sender. This policy allows the entire communication to be unsecured if the other computer is not enabled for IPSec.

Secure Server (Require Security)

Tell students that implementing a Secure Server policy will be covered later in the module and in the lab.

This policy is for computers that always require secure communications. For example, the secure server policy is useful for servers that transmit highly sensitive data, or for a security gateway that protects the intranet from the outside. This policy rejects unsecured incoming communications, and outgoing traffic is always secured. Unsecured communication will not be allowed, even if a peer is not IPSec enabled.

Activating an IPSec Policy

To activate an IPSec policy on a computer:

1. In IP Security Policy Management, click **IP Security Policies on Local Machine**.
2. In the details pane, right-click the policy that you want to assign, and then click **Assign**.

Note You can also assign an IPSec policy to a computer by using Group Policy. For more information about Group Policy, see module 7, “Implementing Group Policy,” in course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

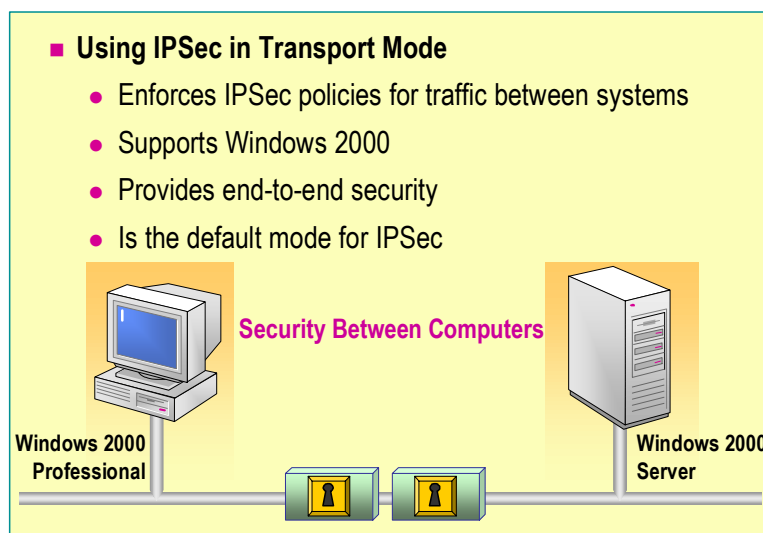
Configuring IPSec for Security Between Computers

Topic Objective

To identify the characteristics of a peer-to-peer IPSec connection.

Lead-in

To create a secure connection between peer computers running Windows 2000, you need to implement IPSec transport mode.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Transport mode creates a secure connection between computers running Windows 2000.

For secured communications between computers running Windows 2000, configure IPSec for transport mode.

Using IPSec in Transport Mode

The transport mode authenticates and encrypts data flowing between any two computers running Windows 2000. The transport mode provides security for the network and can potentially support a secure connection with more than one other computer. Transport mode is the default IPSec mode.

To specify transport mode:

1. Open IP Security Policy Management.
2. In the details pane, right-click the policy that you want to modify, and then click **Properties**.
3. Click the rule that you want to modify, and then click **Edit**.
4. On the **Tunnel Setting** tab, click **This rule does not specify a tunnel**.

Note You can also specify transport mode when you create a new rule by using the Security Rule wizard.

Configuring IPSec for Security Between Networks

Topic Objective

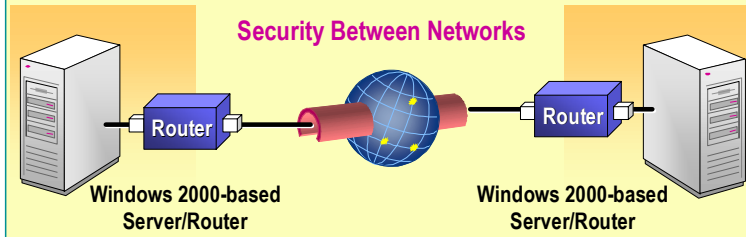
To identify the characteristics of a router-to-router IPSec security connection.

Lead-in

To create a secure connection between two Windows 2000-based routers, implement IPSec tunnel mode.

■ Using IPSec in Tunnel Mode

- Enforces IPSec policies for all Internet traffic
- Supports legacy operating systems predominantly
- Supports point-to-point security
- Specifies tunnel endpoint at both routers



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Tunnel mode creates a secure connection between remote networks.

To create secured communications between remote networks, configure IPSec for tunnel mode. The advantage of tunnel mode is that data is secure between the two tunnel ends, regardless of the ultimate destination. When you configure IPSec for tunnel mode, all communications between networks are secure, without requiring you to configure IPSec on each computer. Tunnel mode does not provide security within each network.

Using IPSec in Tunnel Mode

The tunnel mode for IPSec authenticates and encrypts data flowing within an IP tunnel that is created between two routers. Windows 2000 requires Routing and Remote Access to implement tunnel mode for IPSec.

You enable tunnel mode in IPSec Management. When configuring tunnel mode settings, IPSec requires an IP address for each end of the tunnel.

Delivery Tip

Demonstrate the steps for configuring tunnel mode settings.

To specify an IPSec tunnel:

1. Open IP Security Policy Management.
2. In the details pane, right-click the policy that you want to modify, and then click **Properties**.
3. Click the rule that you want to modify, and then click **Edit**.
4. On the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address**, and then specify the IP address of the tunnel endpoint.

Windows 2000 supports multiple tunnel mode connections, but only one tunnel at a time. Each tunnel connection requires a separate rule.

Note You can also specify an IPSec tunnel when you create a new rule by using the Security Rule wizard.

Customizing IPSec Policies

Topic Objective

To identify the components of IPSec security rules and to illustrate the relationship of policies, rules, and the components of the rules.

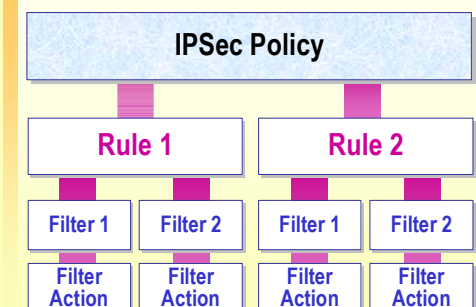
Lead-in

Customize IPSec policies when the default policies do not meet the security needs of your organization.

■ Rule Components

- Tunnel Endpoint
- Network Type
- Authentication Method
- IP Filter List
- Filter Action

■ Default Response Rule



*****ILLEGAL FOR NON-TRAINER USE*****

You can create customized IPSec policies to select which computers require encryption and the security methods that are used for encryption. IPSec policies use rules to govern how and when a policy is invoked. A rule provides the ability to initiate and control secure actions based on the source, destination, and type of IP traffic.

Each IPSec policy may contain one or more rules. Any number of the rules may be active simultaneously. Default rules are provided that encompass a variety of client and server-based communications. You can create new rules or modify the default rules to meet your network requirements.

Rule Components

A rule consists of the following components:

- **Tunnel Endpoint.** Defines the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. There must be two rules to define an IPSec tunnel, one for each direction.
- **Network Type.** Applies to connections configured in Network and Dial-up Connections. Select one of the following options:
 - **All network connections**
 - **Local area network (LAN)**
 - **Remote access**

Delivery Tip

Open the Rules wizard and point out each component as you describe the rule.

- **Authentication Method.** Defines the method for verifying the identity of a user. Windows 2000 supports three authentication methods:
 - **Windows 2000 default (Kerberos V5 protocol).** Uses the Kerberos V5 security protocol for authentication. You can use this method for any clients that are running the Kerberos V5 protocol (whether or not they are Windows-based clients) that are clients in the same forest or from a trusted Kerberos realm.
 - **Use a certificate from this Certificate Authority (CA).** Requires that a trusted CA has been configured. Windows 2000 supports X.509 Version 3 certificates, including CA certificates generated by commercial CAs.
 - **Use this string to protect the key exchange (preshared key).** Specifies a secret, shared key that two users agree upon and manually configure prior to use.
- **IP Filter List.** Defines which traffic will be secured with this rule. You can use the default filters or create policy-specific filters for certain types of IP traffic or specific subnets. Default filters include:
 - **All ICMP traffic**
 - **All IP traffic**
- **Filter Action.** Lists the security actions that will occur when traffic matches an IP filter. The action specifies whether to permit the traffic, block the traffic, or negotiate the security for the given connection. You can specify one or more negotiated filter actions. The filter actions appear as a list, with the first method listed taking precedence. If a filter action cannot be negotiated, the next filter action will be attempted.

To edit the rule properties, click the rule in the **Properties** dialog box for an IPSec policy, and then click **Edit**. To edit the default IP filter list and actions, right-click **IP Security Policies**, and then click **Manage IP filter lists and filter actions**.

Default Response Rule

A computer uses the default response rule to respond to requests for secure communication. If a rule is not defined for secure communication requests, the default response rule is applied and security is negotiated. This rule is designated for all defined policies, but may not be active.

When creating a new policy, the wizard presents the choice of using the default response rule. If the default response rule is activated, the wizard allows the administrator to set the authentication method for the rule.

You can restore the original, predefined configurations, if you modify or delete them beyond regression. Any current modifications that you have made to any of the default policies and rules will be lost.

To restore default policies:

1. Open IP Security Policy Management.
2. In the console tree, click **IP Security Policies Local Machine**, right-click, point to **All Tasks**, click **Restore Default Policies**, and then click **Yes**.

Choosing an IPSec Encryption Scheme

Topic Objective

To list the authentication encryption algorithms and data encryption algorithms.

Lead-in

The method chosen for authentication and packet encryption may vary according to the sensitivity of the information and any government standards.

To Choose an Authentication and Encryption Scheme:

■ Authentication Encryption

- SHA
- MD5

■ Packet Encryption

- 56-bit DES
- 40-bit DES
- 3DES

*****ILLEGAL FOR NON-TRAINER USE*****

The method chosen for authentication and packet encryption may vary according to the sensitivity of the information and any government standards. IPSec offers a variety of authentication and data encryption algorithms.

Explain that unless there are special security requirements, these methods are usually left at the default settings.

To view encryption security methods, open the properties of the selected policy, click the **General** tab, click **Advanced**, and then click **Methods**.

Authentication Encryption

The following table summarizes the authentication encryption choices: Secure Hash Algorithm (SHA) and Message Digest 5 (MD5).

Method	Description
SHA	Federal Information Processing Standards (FIPS) accepted for U.S. government contracts. This high-security method uses a 160-bit key.
MD5	Most widely used method for commercial applications. This high-security method uses a single 128-bit key and has a lower performance overhead.

Packet Encryption

The following table summarizes the data encryption choices.

Method	Description
56-bit DES	Method used for most exported applications and low-security business traffic, such as e-mail. This low-security method uses a single 56-bit key.
40-bit DES	Method supported for application exports to France. This low-security method uses a single 40-bit key. The 40-bit Data Encryption Standard (DES) is not RFC compliant.
3DES	Most secure method. Uses three 56-bit keys. 3DES processes each block three times, using a unique key each time. This high-security method increases processor utilization by a factor of about 2.5 compared with other DES encryption.

Testing an IPSec Policy Assignment

Topic Objective

To identify the tools to use for verifying an IPSec policy assignment.

Lead-in

Before secured data can be exchanged, a security association between the two computers must be established.

- Using the Ping Command to Verify That a Valid Network Connection
- Using IPSec Monitor to Verify That a Policy Has Been Assigned

*****ILLEGAL FOR NON-TRAINER USE*****

Before secured data can be exchanged, a *security association* (SA) between the two computers must be established. In an SA, both computers negotiate how to exchange and protect information. The initiating computer sends an offer list of potential security levels to the responding peers. The responder either sends a reply accepting the offer, or discards the offer and sends back a message indicating that no offer was chosen. If the active policies allow unsecured communications with non-IPSec-capable computers, a *soft* SA is established. If active policies are compatible, a secured, or *hard*, SA is established.

To make sure that an SA can be established and IPSec-secured communication can be successful, use the **ping** command to verify a valid network connection and use IPSec Monitor to verify a valid policy assignment.

Using the Ping Command to Verify That a Valid Network Connection

When testing an IPSec policy assignment, use the ping command to verify a valid network connection. Using ping to verify a valid network connection allows you to separate network problems from IPSec issues.

To verify a valid network connection:

The actual time may be longer if you use a DNS name.

Open a command prompt, type **ping** *IP address* where *IP address* is the IP address of the computer with which you are trying to communicate, and then press ENTER.

If there is a valid network connection, you should receive four replies to the ping. This verifies that you can communicate with the destination IP address. IPSec does not block the ping command if you are using the default policies unmodified.

If there are problems with establishing a secure channel, you will see the response “Negotiating IP Security.” You can expect this response while the secure channel is established, but subsequent output from the ping command should include replies from the remote host.

Important If you create custom policies and do not exempt the Internet Control Message Protocol (ICMP) used by the ping command, using the ping command may present erroneous results.

Using IPSec Monitor to Verify That a Policy Has Been Assigned

IPSec Monitor displays the active security associations on local or remote computers. For example, you can use IPSec Monitor to determine whether there is a pattern of authentication or security association failures, possibly indicating incompatible security policy settings.

To start IPSec Monitor:

- Click **Start**, click **Run**, and then type **ipsecmmon** *ComputerName* where *ComputerName* is the computer that you want to monitor.

When IPSec Monitor opens, you see a message in the lower-right corner indicating whether IPSec is enabled on the computer. For IPSec to be enabled, you must assign a policy. However, no policies are listed in the IPSec Monitor Security Association list unless an SA with another computer is currently active.

Optimizing IPSec Performance

Topic Objective

To describe how the performance of IPSec can be improved.

Lead-in

Here are some things that you might want to consider to improve IPSec performance.

To Ensure High Availability of IPSec Service, Consider:

- **Level of Security Required**
- **Security Requirements of the Computer**
- **Number of IPSec Policy Filter Entries**

*****ILLEGAL FOR NON-TRAINER USE*****

Prior to implementing IPSec in an enterprise network, you should consider the following performance issues.

Level of Security Required

The sensitivity of most data on many enterprise networks may not require the level of security that IPSec provides. When you enable IPSec, processor utilization, IP packet traffic, and IP packet size all increase. You should consider whether a particular host sufficiently benefits from enhanced security before implementing IPSec on that platform.

Note Some vendors offer network adapters that perform the IPSec encryption tasks on the network adapter. Performing the IPSec encryption by using dedicated hardware can significantly increase performance.

Security Requirements of the Computer

Certain data may be sensitive, yet you will only access it with a subset of the computers on the network. Identify the server and client computers requiring access to the sensitive data and enable IPSec on only those computers.

Number of IPSec Policy Filter Entries

IPSec can block unauthorized access through the use of IP filters and negotiation policies. Use wildcard filters to reduce the number of IP filter entries. Negotiation policies should be restrictive enough to ensure that authorized computers have access but unauthorized computers do not. You can design your IPSec configuration with IP filters, negotiation policies, or both.

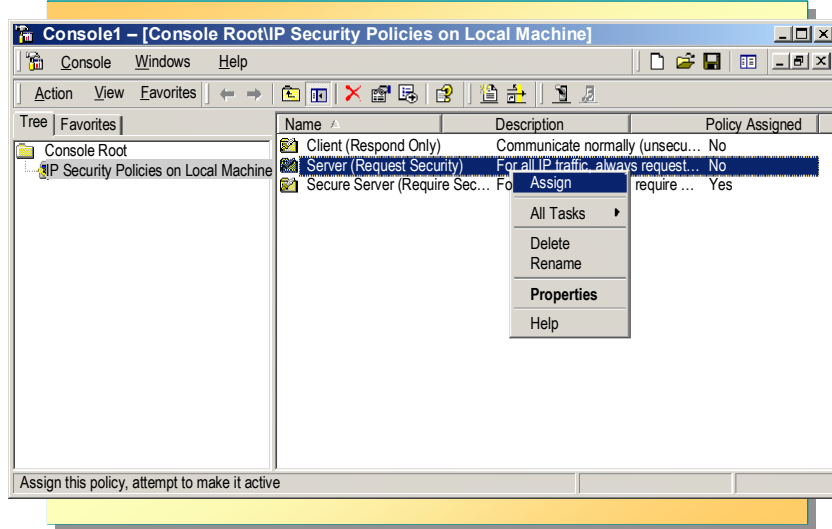
Configuring TCP/IP for Server Security

Topic Objective

To illustrate the interface for configuring TCP/IP for server security.

Lead-in

IPsec at the IP transport level provides protection for server applications and services, without modifying those server applications and services that use IP for transport of data.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

You enable IP Security for TCP/IP by assigning the Secure Server policy.

IPsec at the IP transport level provides protection for server applications and services, without modifying those server applications and services that use IP for transport of data. You can enable IPsec to provide secure end-to-end communication of IP-based traffic on a private network or on the Internet. You enable IP Security for Transmission Control Protocol/Internet Protocol (TCP/IP) by assigning the Secure Server policy. By default, the Secure Server policy is disabled.

To enable IP security for TCP/IP:

1. Open IP Security Policy Management.
2. In the console tree, click **IP Security Policies on Local Machine**.
3. In the details pane, right-click **Secure Server (Require Security)**, and then click **Assign**.

Troubleshooting Network Protocol Security

Topic Objective

To identify the tasks related to troubleshooting network protocol security.

Lead-in

The most common symptom of problems with network protocol security is that two or more computers that are configured to use IPSec cannot communicate with each other.



Review the System and Security Logs for Error Messages



Confirm That a Security Association Is Established Between the Computers



Ensure That the Policies Are Assigned to Both Computers



Ensure That the Policies Are Compatible with Each Other



Ensure That All Changes Are Applied

*****ILLEGAL FOR NON-TRAINER USE*****

The most common symptom of problems with network protocol security is that two or more computers that are configured to use IPSec cannot communicate with each other. When troubleshooting network protocol security, begin by isolating the problem.

Isolating the Problem

When troubleshooting IPSec problems, it is important to isolate the problem. A Communication problem may be due to general network problem or a problem with security settings. Stop the IPSec policy agent on both computers, and then verify communications between computers. If there is a communications problem even with the policy agent stopped, then general network issues are the cause.

Explain that Services helps you manage the services on your computer, set up recovery actions to take place if a service fails, and create custom names and descriptions for services so that you can easily identify them.

To stop the policy agent:

1. Open Services from the **Administrative Tools** menu.
2. In the console tree, right-click **IPSec Policy Agent**, and then click **Stop**.

After you confirm that a problem is related to network security, be sure to restart the IPSec policy agent to continue troubleshooting.

Verifying the IPSec Policy

After you have confirmed that you can communicate with the remote computer, use the following methods to find the problem:

- Review the system logs and security logs for error messages.
- Use IPSec Monitor to confirm that a security association is established between the computers to ensure that the IPSec policy is in effect.
- Use IP Security Policy Management to ensure that the policies have been assigned to both computers.
- Use IP Security Policy Management to review the policies on both computers and ensure that the policies are compatible with each other.
- Restart the IPSec Security Monitor to ensure that all changes that you have made are applied.

Note For more information about troubleshooting IPSec, see “Troubleshooting IP Security” in Windows 2000 Help.

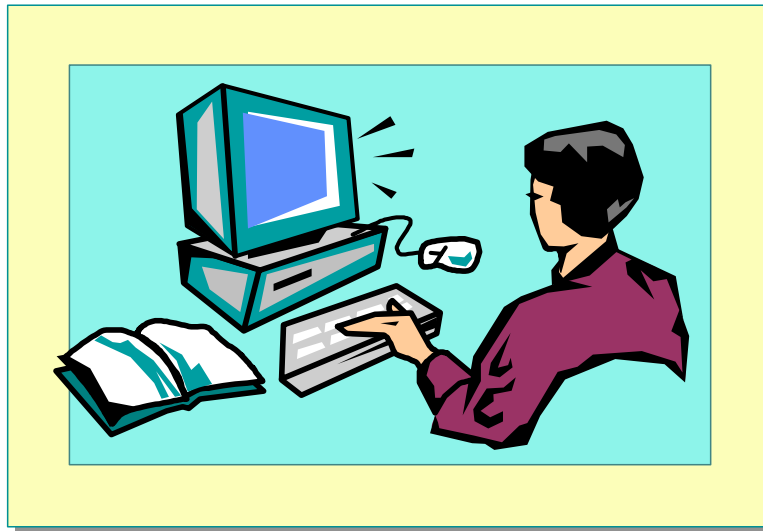
Lab A: Configuring TCP/IP for Secure Connections by Using IPSec

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will secure network traffic by using IPSec



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Configure an IPSec policy.
- Assign an IPSec policy.

Prerequisites

Before working on this lab, you must have:

- Knowledge of how IPSec works.
- Knowledge of the role of IPSec policies in securing network traffic.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server and configured as a domain controller.
- A partner with a similarly configured computer.
- Certificates that are assigned to your computer and your partner's computer. Both certificates must be from CAs in a certification authority path that both student computers trust.
- The IP address of the instructor's computer.

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Scenario

Your organization is working on a project that includes business partners. Work on the project requires extreme confidentiality. Your business partners will access data on some of your servers by using the Internet. You must ensure that all network traffic between the computers in your organization and your business partners' computers is encrypted. Your organization has an existing Public Key Infrastructure (PKI) that includes CAs. You have also issued certificates to all of the computers in your organization that your business partners will access and to the computers that your business partners will use to access your servers.

Estimated time to complete this lab: 45 minutes

Exercise 1

Creating and Assigning an IPsec Policy

Scenario

As part of a joint development project with a business partner, you must ensure that all network traffic between servers on your network and your partners' computers is encrypted. To ensure this, you must use IPsec and computer certificates that you have issued to all computers.

Goal

In this exercise, you will work with a partner to configure and test an IPsec policy for two computers by using certificates.

Tasks	Detailed Steps
1. Use the Ping utility to test communications with your partner.	a. Log on as <code>administrator@domain.nwtraders.msft</code> (where <i>domain</i> is the name of your domain) with a password of password. b. At a command prompt, type ping 192.168.z.y (where <i>z</i> is your assigned classroom number and <i>y</i> is your partner's student number), and then press ENTER.  <i>You should receive four replies from your partner's computer.</i> c. Minimize the command prompt window.
2. Add the IP Security Policy Management snap-in to an MMC console. Configure IP Security: Tunnel Endpoint: no tunnel Network Type: all connections Authentication Method: certificate from the same certification authority that your partner selects IP Filter List: All IP Traffic Filter Action: Require Security	a. Click Start, and then click Run. b. In the Open box, type mmc and then click OK. c. Maximize the Console Root window. d. In the Console1 – [Console Root] window, on the Console menu, click Add/Remove Snap-in. e. In the Add/Remove Snap-in dialog box, click Add. f. In the Add Standalone Snap-in dialog box, click IP Security Policy Management, and then click Add. g. In the Select Computer dialog box, verify that Local computer is selected, and then click Finish. h. In the Add Standalone Snap-in dialog box, click Services, and then click Add. i. In the Services dialog box, verify that Local computer is selected, and then click Finish. j. Click Close to close the Add Standalone Snap-in dialog box, and then click OK to close the Add/Remove Snap-in dialog box. k. In the console tree, click IP Security Policies on Local Machine. l. In the details pane, right-click Secure Server (Require Security), and then click Properties. m. In the Secure Server (Require Security) Properties dialog box, click Add.

Tasks	Detailed Steps
2. (continued)	n. Complete the Security Rule wizard by using the following information. Accept the defaults where no information is provided (accept the defaults where no information is provided): Tunnel Endpoint page: Verify that This rule does not specify a tunnel is selected. Network Type page: Verify that All network connections is selected. Authentication Method page: Click Use a certificate from this Certificate Authority (CA), click Browse, and then click <i>server CA</i> (where <i>server</i> is the name of a computer that holds a trusted root CA, which normally is your computer or your partner's computer). Ask your instructor if you are unsure about which CA to select. IP Filter List page: Click All IP Traffic. Filter Action page: Click Require Security. o. Click Finish to close the wizard.  <i>Four rules appear in the IP Security Rule box.</i> p. In the Secure Server (Require Security) Properties dialog box, clear the check boxes for all of the rules except the one that displays Certificate in the Authentication column. q. Click Close to close the Secure Server (Require Security) Properties dialog box.
	Note: You have just created a new security rule for the Secure Server policy. The rule uses the default settings, with the exception of using a certificate.
2. (continued)	r. In the details pane, right-click Secure Server (Require Security) , and then click Assign .
	Wait until your partner has completed the previous procedures before starting the following procedure.
3. Test IPSec by using the ping command and IP Security Monitor.	a. In the console tree, click Services (Local), and in the details pane, right-click IPSEC Policy Agent, and then click Restart. b. Minimize the Console1 window. c. Restore the command prompt window, type ping 192.168.x.y (where <i>x</i> is your assigned classroom number and <i>y</i> is your partner's student number), and then press ENTER.  <i>One or both partners will see "Negotiating IP Security" messages. If you receive "Negotiating IP Security" messages, repeat the ping command until you receive replies from your partner's computer.</i> d. At the command prompt, ping the IP address of the instructor computer several times.  <i>There is no reply from the instructor computer because that computer is not configured for IPSec.</i> e. At the command prompt, type ipsecmon and then press ENTER.  <i>IP Security Monitor starts, showing the IPSec activity.</i> f. In IP Security Monitor, click Options.

Tasks	Detailed Steps
3. (continued)	g. In the IP Security Monitor Options dialog box, in the Refresh Seconds box, type 1 and then click OK. h. Arrange the windows on your screen so that you can see the IPSec Statistics box in IP Security Monitor and the command prompt window. i. Ping your partner's computer a few more times, while viewing the results in the IPSEC Statistics box in IP Security Monitor.  Notice that the IPSEC Statistics box displays an active association and indicates that the number of confidential and authenticated bytes sent and received is increasing while you are using the ping command. j. Close IP Security Monitor, close the command prompt window, and then restore the Console1 window.
4. Remove the Security Association.	a. In the console tree, click IP Security Policies on Local Machine, and in the details pane, right-click Secure Server (Require Security), and then click Un-assign.  The Policy Assigned status will change from Yes to No, indicating that there are no active IP Security policies. b. In the console tree, click Services (Local), and in the details pane, right-click IPSEC Policy Agent, and then click Restart. c. Close the Console1 window without saving the changes, and then log off.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to IPSec
- Implementing IPSec
- Configuring TCP/IP for Server Security
- Troubleshooting Network Protocol Security

*****ILLEGAL FOR NON-TRAINER USE*****

1. How can IPSec prevent network security breaches that are caused by network monitoring and address spoofing?

IPSec includes protocols and services for encryption (which prevents network monitoring) and authentication (which prevents address spoofing).

2. How do the predefined policies Server (Require Security) and Server (Request Security) differ from each other?

A computer that is configured with Server (Request Security) tries to negotiate secure communication with a client computer but uses unsecured communication if security settings cannot be negotiated successfully. A computer that is configured with Server (Require Security) does not allow unsecured communications, even if a peer is not IPSec enabled.

3. When do you use transport mode, and when do you use tunnel mode?

You use transport mode to establish a secure connection between two computers. You use tunnel mode between routers to establish a secure connection between two networks.

4. What are the authentication methods that you can use for IPSec?

Windows default (Kerberos V5), certificates from a CA, and a preshared key.

5. When troubleshooting IPSec, how do you determine whether a problem is caused by security settings or by general network problems?

Disable network security on both computers that you are testing and determine whether you can successfully communicate without network security enabled.

