Objectives

To know more about IPsec.
To configure and test IPsec on windows server.

Introduction:

A number of approaches to providing Web security are possible. The various approaches that have been considered are similar in the services they provide and, to some extent, in the mechanisms that they use, but they differ with respect to their scope of applicability and their relative location within the TCP/IP protocol stack.

One way to provide Web security is to use IP Security (Figure 1a). The advantage of using IPSec is that it is transparent to end users and applications and provides a general-purpose solution.

IPsec is a collection of protocols and mechanisms that provide confidentiality, authentication, message integrity, and replay detection at the IP layer.

Conceptually, think of messages being sent between two hosts as following a path between the hosts. The path also passes through other intermediate hosts. IPsec mechanisms protect all messages sent along a path. If the IPsec mechanisms reside on an intermediate host (for example, a firewall or gateway), that host is called a security gateway.
Applications of IPSec

IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include the following:

- A typical scenario of IPSec usage. An organization maintains LANs at dispersed locations. Nonsecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPSec protocols are used. These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world. The IPSec networking device will typically encrypt and compress all traffic going into the WAN, and decrypt and decompress traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN. This scenario is shown in figure 2.

- Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.
Establishing extranet and intranet connectivity with partners: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security.

The principal feature of IPSec that enables it to support these varied applications is that it can encrypt and/or authenticate all traffic at the IP level. Thus, all distributed applications, including remote logon, client/server, e-mail, file transfer, Web access, and so on, can be secured.

**IPSec modes:**

IPSec has two modes:

1. Transport mode encapsulates the IP packet data area (which is the upper layer packet) in an IPsec envelope, and then uses IP to send the IPsec-wrapped packet. The IP header is not protected. Transport mode is used when both endpoints support IPsec. Show in figure 3 left.

2. Tunnel mode encapsulates an entire IP packet in an IPsec envelope and then forwards it using IP. Here, the IP header of the encapsulated packet is protected. Tunnel mode is used when either or both endpoints do not support IPsec but two intermediate hosts do. Show in figure 3 right.

---

**Figure 3** The packet on the left is in transport mode, because the body of the packet is encrypted but its header is not. The packet on the right is in tunnel mode, because the packet header and the packet body are both encrypted. The unencrypted IP header is used to deliver the encrypted packet to a system on which it can be decrypted and forwarded.
Benefits of IPSec
These are some benefits of IPSec:

- When IPSec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- IPSec in a firewall is resistant to bypass if all traffic from the outside must use IP, and the firewall is the only means of entrance from the Internet into the organization.
- IPSec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router. Even if IPSec is implemented in end systems, upper-layer software, including applications, is not affected.
- IPSec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- IPSec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

Security Associations
A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA). An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it. If a peer relationship is needed, for two-way secure exchange, then two security associations are required. Security services are afforded to an SA for the use of AH or ESP, but not both.

A security association is uniquely identified by three parameters:
- Security Parameters Index (SPI): A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

- IP Destination Address: Currently, only unicast addresses are allowed; this is the address of the destination endpoint of the SA, which may be an end user system or a network system such as a firewall or router.

- Security Protocol Identifier: This indicates whether the association is an AH or ESP security association.

Hence, in any IP packet, the security association is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP).
Lab Experiment

Requirements:
We need two machine in this lab ; the first that runs windows server 2003, and the other runs windows XP work as client.

Part1 : Using IPSec Default Policies :
In this part we examine the default IP Security (IPSec) policies in windows server 2003. And the next part show easy steps to create custom policy.


We have three default policies :

- **Secure Server (Require Security)**: For all IP traffic, always require security using Kerberos trust. Do NOT allow unsecured communication with untrusted clients.

- **Client (Respond Only)**: Communicate normally (unsecured). Use the default response rule to negotiate with servers that request security. Only the requested protocol and port traffic with that server is secured.

- **Server (Request Security)**: For all IP traffic, always request security using Kerberos trust. Allow unsecured communication with clients that do not respond to request.

Figure 5 illustrate default IPSec policies.

From step 2- 5 we test Secure Server policy and 6-7 testing client policy.

2. Right-click Secure Server and choose Assign. The policies should look like Figure

3. From Command Prompt, Type `gpupdate` and to ensure that the policy is updated on the domain controller.

4. In Windows XP Log on using an account you have not logged in with before (We need an account that not logging before because of credential-username and password- caching).

5. The result that you cannot logon, and you receive an error that the your domain is not available because the client computer is not configured to use IPSec and the domain controller will not accept unsecure connections. this is shown in figure 4.


7. In Windows XP try to Log on using an account you have not logged in with before ; the difference here is you can successfully logging.
Q: According to your information is the policy a transport mode or tunnel mode policy? **Transport mode**

![Figure 4](image1.png)

Figure 4 unsuccessful log on process when secure server default policy is configured

![Figure 5](image2.png)

Figure 5
Part 2: Implementing Packet Filtering with IPSec

IPSec allows you to create filters that permit, block, or negotiate communication. You can use a block action on a filter to prevent traffic that meets the filter criteria from being processed by the computer to which the policy applies.

Note: if any step does not specified keep the default configuration and click next.

2. Right click and choose Create IP Security Policy.
3. The IP Security Policy Wizard will open. Click Next and Name your policy.
4. Keep Active the default response rule checked and click Next.
5. In the next window we will configure Default Response Rule Authentication Method, we can use default authentication method Kerberos V5, or a certificate previously defined from Certificate Authority, or Pre-shared key. Also we can use multiple authentication methods by adding another method later. Now keep the default authentication method, Active Directory default (Kerberos V5 Protocol) and click Next.
6. Keep Edit properties if you want to add new authentication method.
7. Now you need to configure additional rules. Click Add.
8. The Create IP Security Rule Wizard will open. Click Next to continue past the Welcome screen, IP Security Rule Wizard shown in figure 6.
9. Keep This rule does not specify a tunnel selected and click Next.
10. From select your network type select All network connections.
11. On the IP Filter List screen, click Add to display the IP Filter List shown in figure 7, Click Add to open the IP Filter Wizard.
12. Type suitable description for your filter, as example Block port 20 traffic.
13. Determine source address and destination address and port (or protocol); as an example if we want to block FTP access to my network we use Any IP Address in the IP Traffic Source dialog box. and My IP Address in the destination, Select Other as the protocol type and type 20 in the field.
14. Now we must select the action we want to perform for the selected IP filter; we have Permit, Request security, Require security filter actions by default and we can define new action.
15. Click Add in the Filter Action dialog box to launch the IP Security Filter Action Wizard. Type Block as the name and click Next, Select Block on the next screen.
16. Close all opened dialog boxes.
A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule’s IP filter list.

A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list:

- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

---

**Figure 6 IP Security Rule Wizard**

---

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

**Figure 7 IP Filter List**
**Modify an IPsec policy**

IPsec allows you to configure filters that negotiate security and allow a client to select an authentication protocol and an encryption protocol. In this part of the lab, we modify the IPsec policy we created in part 2 to require 3DES encryption and Kerberos or preshared key authentication.

1. From Domain Security Policy. Open the Properties of the policy that created in the previous part.
2. Select the filter previously created in part 2 and click Edit.
3. From Filter Action tab, Click Add to launch the IP Security Filter Action Wizard. Then Click Next to continue past the Welcome screen.
4. Name the filter action and click Next.
5. Keep Negotiate security selected and click Next.
6. Keep Do not communicate with computers that do not support IPsec selected and click Next. With this option, Legacy computers and computers that have not been configured to respond to IPsec requests will not be able to communicate using FTP or any protocol or service you configure to use IPsec. We can use Allow unsecured communication with non-IPsec-aware computers option to allow unsecured communication only with computers that do not support IPsec.
7. Keep Integrity and encryption selected and click Next then Finish. **Note that:** 3DES is the encryption algorithm used and integrity algorithm used is SHA1. As shown in figure 8.
8. Click OK to close the properties for the filter action.
9. Select the new action to be used in the IPsec policy.

![Figure 8](image)
10. From **Authentication Methods** tab, Click Add and Select Use this string (preshared key).

11. Type any key, and Click OK. You need also use the same key at the client to allow secure connection encrypted by the specified key.

**Note that:** Now we have two authentication methods, Kerberos authentication method will be tried first in our example then preshared key, we can change order of the authentication methods.

Exercise:

Create IP Security Policy as the following:

1. use pre-shared key "IUG123456" and any user certificate as an alternate authentication method.

2. filter data that comes on port 23 telnet port from all users that not configure to use IPSec, and block traffic for port 53 for all users.