Assignment 1 - The Simenar

Mohammed Altemimi (Microsoft Member)
dept. FTSM
Mohammed Alaa Hussein Altemimi
UKM University , Malaysia
goodprogrammer2005@yahoo.com

Securing Network Traffic by Using IPSec and Certificates - Implementing IPSec What Is IPSec? (Define IPSec, encryption, and decryption) How IPSec Secures Traffic (Define security association and Internet Key Exchange) What Is an IPSec Security Policy? (Explain that an IPSec Security policy consists of a set of rules that determine how IPSec works) How IPSec Policies Work Together Guidelines for Balancing Security and Performance (Discuss how to apply the guidelines to properly balance the need for security without affecting performance) How to Assign or Unassigned an IPSec Policy on a Computer Demonstrate how to add an IPSecurity Management Console and then assign or unassign an IPSec policy for a local computer policy. Demonstrate how to assign and unassign an IPSec policy for an Active Directory-based group policy.

- Implementing IPSec with Certificates What Is a Certificate? Common Uses of Certificates Why Use Certificates with IPSec to Secure Network Traffic? Multimedia: Certificate Enrollment How to Configure IPSec to Use a Certificate

- Monitoring IPSec IP Security Monitor Guidelines for Monitoring IPSec Policies How to Stop and Start the IPSec Services How to View IPSec Policy Details

1. Introduction

You can secure Network Traffic by us e IPSec So that unauthorized users or application can't access private data on TCP/IP protocol.

A significant amount of data that passes over a local area network (LAN) is in a form that could be easily captured and interpreted by a protocol analyzer connected to the network. If any data is captured, an attacker could potentially modify and retransmit the modified data over the network. To secure the data that is transmitted over the network from these types of attacks, you can encrypt network data by using IPSec. IPSec allows you to define the scope of your encryption. For example, you can encrypt all network communication for specific clients or for all clients in a domain.

[IPSec] IPSec is a suite of protocols that allows secure, encrypted communication between two computers over an unsecured network. IPSec has two goals: to protect IP packets, and to provide a defense against network attacks. Configuring IPSec on sending and receiving computers enables the two computers to send secured data to each other. IPSec secures network traffic by using encryption, decryption, and data signing. You use IPSec policies to configure IPSec. A configuration policy defines the type of traffic that IPSec examines, how that traffic is secured and encrypted, and how IPSec peers are authenticated. There are default IPSec policies that you can use, or you can create a custom policy. You can configure only one IPSec policy at a time for a single computer.

[Definition] IPSec is an industry-defined set of standards that verifies, authenticates, and encrypts data at the IP packet level. IPSec is used to provide data security for network transmissions. Encryption is the process of encoding a message or data through a mathematical key in a manner that hides its substance from anyone who does not possess the mathematical key. Decryption is the reverse process of encryption. Decrypting data involves applying the appropriate mathematical key to decode the message or data so that it is restored to its original content.

[Purpose of IPSec] IPSec is used to provide data security for network transmissions. The administrator sets a series of rules called an IPSec policy. These rules contain filters that specify what types of traffic require encryption, digital signing, or both. Then, every packet that the computer sends is assessed to find whether it matches the conditions of the policy. If it matches the policy conditions, it can be either encrypted or signed according to the policy. This process is transparent to the user and applications that initiate the data transmission. Because IPSec is contained inside a standard IP packet, it can travel through a network without requiring special configuration on the devices in between the two hosts. IPSec cannot encrypt some types of traffic, such as broadcasts, multicasts, and Kerberos protocol packets.

[Benefits of IPSec] The major benefit of IPSec is that it provides totally transparent encryption for all protocols from Open Systems Interconnection (OSI) model layer 3 (network layer) and higher. IPSec provides: - Mutual authentication before and during communications. IPSec forces both parties to identify themselves during the communication process. - Confidentiality through encryption of IP traffic and digital authentication of packets. IPSec has two modes: Encapsulating Security Payload (ESP), which provides encryption by using one of a few different algorithms, and Authentication Header (AH), which signs the traffic but does not encrypt it. - Integrity of IP traffic by rejecting modified traffic . Both ESP and AH verify the integrity of all IP traffic. If a packet has been modified, the digital signature will not match, and the packet will be discarded. ESP encrypts the source and destination addresses as part of the payload. - Prevention against replay attacks. Both ESP and AH use sequence numbers, so that any packets that are captured for later replay would be using numbers out of sequence. Using sequenced numbers ensures that an attacker cannot reuse or replay captured data to establish a session or gain information illegally. Using sequenced numbers also protects against attempts to intercept a message and then use the identical message to illegally gain access to resources, possibly months later.

[Example] Because the capturing of confidential information can compromise an organizations success, an organization needs to have reliable network security for sensitive information, such as product data, financial reports, and marketing plans. You can use IPSec to ensure secure and private communications within a network, intranet, or extranet including workstation-to-server and server-to server communications.

[How IPSec works] IPSec configuration is set through either a local policy or a group policy in the Active Directory directory service: 1. IPSec policies are delivered to all targeted computers. The policy tells the IPSec driver how to behave and defines the security associations that can be established. Security associations govern what encryption protocols are used for what types of traffic and what authentication methods are negotiated. Define: Internet Key Exchange (IKE) is a protocol that establishes the security association and shared keys necessary for two parties to communicate by using IPSec. 2. The security association is negotiated. The Internet Key Exchange (IKE) module negotiates the security association. IKE is a combination of two protocols: the Internet Security Association and Key Management Protocol (ISAKMP) and the Oakley Key Determination Protocol. If one client requires certificates for authentication and the other client requires the Kerberos protocol, IKE will not be able to establish a security association between these two computers. If you look at the packets in Network Monitor, you will see ISAKMP packets, but you will not see any subsequent AH or ESP packets. 3. IP packets are encrypted. After the security association is established, the IPSec driver monitors all IP traffic, compares traffic to the defined filters, and if directed to, either encrypts or signs the traffic.

An IPSec Security policy consists of one or more rules that determine IPSec behavior. You implement IPSec by setting a policy. Each policy can contain several rules, but you can only assign a single policy at any one time on any computer. You must combine all desired rules into a single policy. A filter. The filter tells the policy what type of traffic to apply the filter action to. For example, you can have a filter that identifies only Hypertext Transfer Protocol (HTTP) traffic or File Transfer Protocol (FTP) traffic.

A filter action. The filter action tells the policy what to do if the traffic matches the filter. For example, you can tell IPSec to block all FTP traffic but require encryption for all HTTP traffic. The filter action can also specify which hashing and encryption algorithms the policy should use. An authentication method. There are three possible authentication methods: certificates, the Kerberos protocol, and a preshared key. Each rule can specify multiple authentication methods.

Kerberos authentication:- is the default setting for all three default policies. Kerberos protocol works for computers in the same Active Directory forest, but if a computer is not a member of the forest, the computers cannot negotiate authentication. Also, if computer B is modified to use only certificates for authentication for all IP traffic, no security association will be established. It is possible to change computer B to require either the Kerberos protocol or certificates. As long as one authentication method matches, authentication can occur.

[Mode] Encapsulation security payload. Authentication Header. CPS: cryptographic protocol services, located at local machine and responsible for generating public key and private key at client side. The policy agent is IPSec services located at client under services.

[Implementing IPSec with Certificates] IPSec relies on mutual authentication to provide secure communications. Because IPSec is an industry standard, this authentication may need to occur between systems that do not share a centralized Kerberos protocol authentication infrastructure. X.509 certificates provide another means of authentication for IPSec that is standards-based and can be used if a trusted Public Key Infrastructure (PKI) is in place. This lesson describes how you can use public key certificates for authentication to provide trust and secure communication in your network.

What Is a Certificate:- Certificates are an electronic credential that authenticates a user on the Internet and intranets.

Definition:- An X.509 certificate, also sometimes called a digital certificate, is an electronic credential that is commonly used for authentication and secure exchange of information on open networks, such as the Internet, extranets, and intranets. A certificate securely binds a public key to the entity that holds the corresponding private key. For example, you can encrypt data for a recipient with their public key, trusting that only the recipient has the private key that is required to decrypt the data. A certificate issuer, called a certification authority (CA), digitally signs certificates. The certificates can be issued for a user, a computer, or a service, such as IPSec.

[Benefit of certificates] One of the main benefits of certificates is that hosts no longer have to maintain a set of passwords for individual subjects who need to be authenticated as a prerequisite to access. Instead, the host merely establishes trust in a CA that issues certificates.

[Purpose of a certification authority] A CA is responsible for authenticating and validating the keys for encryption, decryption, and authentication. After a CA verifies the identity of a key holder, the CA distributes the public keys by issuing X.509 certificates. X.509 certificates contain the public key and a set of attributes. A CA can issue certificates for specific functions, such as secure e-mail or IPSec, in addition to general purpose certificates.

[Certificate contents] A certificate contains the following information: The public cryptographic key from the certificate subjects public and private key pair. Information about the subject that requested the certificate. The user or computers X.500 distinguished name. The e-mail address of the certificates owner. Details about the CA. Expiration dates. A hash of the certificate contents to ensure authenticity (digital signature).

[Uses of certificates] Many organizations install their own CAs and issue certificates to internal devices, services, and employees to create a more secure computing environment. Therefore, an employee of an organization may have several certificates issued by more than one CA.

[Purpose of certificates] Using certificates from a trusted CA as the method of authentication between two IPSec hosts allows an enterprise to interoperate with other organizations that trust the same CA. You can also use certificates to enable Windows Routing and Remote Access service to securely communicate over the Internet with a third-party router that supports IPSec. However, because certificates are more complex than either preshared keys or the Kerberos protocol, they require more administrative planning. Certificates are just one component of a PKI solution. Although PKI requires planning and management resources, it crosses enterprise borders to allow the bond of identity and trust to be established between organizations.

[Kerberos protocol and preshared keys] The other two methods for authentication between two IPSec hosts include: Kerberos protocol. For traffic between computers in the same forest, using the default Kerberos protocol authentication is the simplest authentication for IPSec and does not require any configuration. The Kerberos protocol is a component of Active Directory, so it is part of an enterprise domain structure. However, for clients that do not support the Kerberos protocol or for clients that are not part of the Active Directory structure, using some another means of authentication is required, such as either a preshared key or X.509 certificate.

Preshared keys. A preshared key is a large random text string that is used as a password between two IPSec hosts. Preshared keys are not considered as secure as the Kerberos protocol or certificates because they are stored in clear text in the IPSec policy. An attacker could gain administrative access to the policy and then obtain the preshared key. Preshared keys also do not scale well to multiple computer configurations.

September 1, 2009

2.

Acknowledgment

The Researcher Mohammed Altemimi would like to thank Dr. Mohd Zamri and all My classmate to listen ...

References

[1] Microsoft, *A Guide to Network Infrastrucure LaTeX*, 3rd ed., .