Implementing and Managing Security for Network Communications

**Terms you’ll need to understand:**
- Internet Protocol Security (IPSec)
- Authentication
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- IPSec certificates

**Techniques you’ll need to master:**
- Planning and IPSec deployment
- Configuring IPSec policies
- Deploying and managing IPSec policies
You should always maintain secure communications within your network and between networks to whatever degree possible. Internet Protocol Security (IPSec) allows you to control security using flexible policies to adapt to any network. IPSec secures data in the private and public environments of your network by providing a strong cryptography-based defense.

In this chapter, we discuss securing your network with IPSec, which includes the following:

➤ Planning an IPSec deployment
➤ Configuring IPSec policies
➤ Deploying and managing IPSec policies

Planning an IPSec Deployment

One of the best features of IPSec is its flexibility. Unfortunately, that’s a double-edged sword when it comes to network design. IPSec can be configured for the needs of almost any network, but many decisions must be made regarding its configuration. Some decisions are made for you by the way in which you are using IPSec or by the types of client operating systems that you are running on your network; other decisions are made by you. We now discuss the steps that you must take to deploy IPSec, which include the following:

➤ Deciding which IPSec mode to use
➤ Planning authentication methods for IPSec
➤ Securing authentication with IPSec
➤ Testing the functionality of existing applications and services

Deciding Which IPSec Mode to Use

This decision is rather easy because it has already been made for you based on the way you are using IPSec. Basically, two different types of communications exist that you need to secure—communications within a network and communications between networks. You choose one of two modes of IPSec security—transport mode or tunnel mode—based on the type of communication you need to make secure.
Transport Mode
You can use IPSec in *transport mode* to secure communications between two computers on the same network. This can be server-to-server or server-to-client communications. Once configured, IPSec provides end-to-end security based on the *authentication* and encryption settings that you apply. Figure 3.1 illustrates the concept of IPSec transport mode.

![IPSec Transport Mode](image1)

*Figure 3.1* IPSec transport mode provides secure communication from endpoint to endpoint within a network.

Tunnel Mode
You can use IPSec in *tunnel mode* to secure communications between two networks. You define the endpoints of the tunnel, and the system maintains a secure connection between the endpoints. The endpoints are generally router interfaces. You can specify the types of encryption and authentication protocols that will be required for all traffic. Figure 3.2 illustrates the concept of IPSec tunnel mode.

![IPSec Tunnel Mode](image2)

*Figure 3.2* IPSec tunnel mode provides for secure communications between two networks.
Planning Authentication Methods for IPSec

Authentication is the process of a network entity proving its identity in a confidential manner. Because authentication must be confidential, computers need to be able to authenticate to each other using a secure method. IPSec uses three main methods of authentication. You make your choice based on the capabilities of your servers and clients and the requirements of your organization. The three main methods from which you can choose are as follows:

➤ Kerberos
➤ Certificates
➤ Preshared key

Kerberos

Kerberos is the default authentication method for Windows 2000 Server and Windows Server 2003. With Kerberos, the client must prove its identity to the server and the server must also prove its identity to the client. This is referred to as mutual authentication. Kerberos can only be used with Windows 2000 Professional and later clients. You should use Kerberos when all of your clients are in the same domain or Kerberos realm and can authenticate using Kerberos and when you want to use a method that requires the least administrative effort.

Figure 3.3 illustrates that Kerberos is the default protocol in the IP security policy.

When an exam question specifies an authentication method that requires the least administrative effort, and all of the clients and servers are Windows 2000, Windows Server 2003, or Windows XP Professional, you should first determine whether all of the clients are in the same domain. If so, you should use the default Kerberos authentication method. If not, then other methods will have to be considered.

Certificates

As we discussed earlier, certificates are a method of granting access to a user based on the user's unique identification and whether the user possesses the right keys or algorithms to “unlock” the appropriate doors. You issue a certificate to a computer as a means for it to hold the key and as a means for you to track that the computer has the key. You can stipulate in an IPSec policy, as shown in Figure 3.4, that the computer or user must use a certificate (Secure Server) or that it should use a certificate if it has one (Server).
Implementing and Managing Security for Network Communications

Figure 3.3  Kerberos is the default authentication protocol for Windows 2000 Server and for Windows Server 2003 IPSec.

Figure 3.4 illustrates the default policies that are included in Windows Server 2003. Microsoft recommends that you create your own policies by modifying the default policies or by starting from scratch and using the Create IP Security Rule Wizard. Depending on your settings, you will create a policy that must be met in its entirety for communications to continue or a policy that can be negotiated between computers.

**Preshared Key**

A *preshared key* is a *string* that you can use to authenticate computers as a last resort. You should not use a preshared key if any other authentication method is available. A preshared key is a symmetric key, which means that the same key that is used to encrypt can also be used to decrypt. You should configure the same string on all computers that you want to authenticate.

The main problem with a preshared key is that you have no way of knowing whether the key is discovered. Also, the key is not specific to any individual. Therefore, an attacker could use the key to authenticate to a network and you could not trace the attack back to an individual. In addition, the preshared key is stored in the Registry in plain text form. It can be configured from the Authentication Methods tab in the properties of an IPSec policy as shown in Figure 3.5.
Chapter 3

Figure 3.4 You can require or request certificates as part of an IPSec policy.

Figure 3.5 You can use a string to configure a preshared key when no other authentication options exist.

Security Authentication with IPSec

As mentioned previously, your goal is to allow computers to authenticate to each other without anyone else being able to see the process. To facilitate
this, the authentication process must be encrypted. Two main protocols can be used when authenticating with IPSec. These are Secure Hash Algorithm (SHA) and Message Digest 5 (MD5). In addition, after authentication takes place, you can use multiple levels of encryption for the data itself. You should be familiar with the following terms and settings for IPSec encryption. These settings are illustrated in Figure 3.6 and can be located by clicking the General tab of an IPSec policy, then the Settings button, and finally the Methods button.

➤ Secure Hash Algorithm (SHA)
➤ Message Digest 5 (MD5)
➤ Data Encryption Standard (DES)
➤ Triple DES (3DES)

![Figure 3.6](image)

Figure 3.6 You can choose the type of encryption used by IPSec during authentication and during data transfer.

**Secure Hash Algorithm (SHA)**

Secure Hash Algorithm (SHA) is the accepted standard for securing authentication of computers working with government contracts. It is used as part of the Federal Information Processing Standard (FIPS). SHA is a very high-security method that uses a 160-bit encryption key.

**Message Digest 5 (MD5)**

Message Digest 5 (MD5) is used for most commercial applications. You can use MD5 to secure authentication as well as data. This high-security method
uses a 128-bit encryption key. It also has a lower performance overhead than that of SHA.

**Data Encryption Standard (DES)**
Data Encryption Standard (DES) is the lowest encryption strength of the Diffie-Hellman algorithms. It produces only a 56-bit key and is therefore not recommended for use in a high-security environment.

**Triple DES (3DES)**
Triple DES (3DES) is a much stronger Diffie-Hellman algorithm than DES, and produces a 168– to 2048-bit key. It is recommended for use in medium-to high-security networks.

**Testing the Functionality of Existing Applications and Services**
Remember, the reason that you originally decided to use security methods was to protect the integrity and the productivity of the network. For this reason, you should always test the applications and services that you are running on your network to make sure that they can still function with the IPSec rules that you have configured. There are many reasons that an application could cease to function or function with errors. Most of these involve the fact that IPSec rules can be used to filter traffic. Sometimes these filters, as indicated in the following list, can cause unexpected results:

- Filtered ports
- Filtered IP addresses
- Filtered protocols

You can use the IP Filter Wizard (see Figure 3.7) to create multiple filters in an IPSec policy rule. If you use more than one filter in a single IPSec policy rule, be aware that the order that the filters are processed in is not necessarily the order in which you are viewing them. Instead, the IPSec Policy Agent reads the policy, and the filters are processed into one ordered list that is sorted from the most to the least specific. You can use the IPSec Monitor console to view the filters sorted by their weight. If you change or delete a filter, the IPSec Policy Agent reorders the filters based on what remains. Because of this, you should always test applications that use IPSec after applying IPSec and after changing any filters. You should use a test lab, if one
is available, to test the effect of IPSec rules before assigning them in a production environment.

Figure 3.7 You can use the IP Filter Wizard to create multiple filters in an IPSec policy rule.

IPSec can now function through some Network Address Translation (NAT) infrastructures. As long as the version of NAT is compliant with the latest RFC and is configured to allow User Datagram Protocol (UDP) traffic, the Internet Key Exchange (IKE) protocol will detect the presence of NAT and use UDP-ESP encapsulation to allow the traffic to pass through.

**Configuring IPSec Policies**

You should understand that IPSec is designed to be an end-to-end security model that secures traffic between clients and servers. The IP address of the computer does not necessarily have to be the entity that is considered; rather, the system that uses the IP address is validated through an authentication process. This allows you to deploy IPSec to a computer, domain, site, or any container within your Active Directory (AD).

In addition, because there are many ways to authenticate, IPSec can be used to secure local area network (LAN) communications, wide area network communications, and remote access communications as well. This is accomplished through the configuration of IPSec policies that contain rules and filters. The rules and filters that you use will depend on what you are securing and how much protection it requires. You should be familiar with the following configuration options using IPSec:

- Transport mode
- Tunnel mode
- IPSec policy rules
Transport Mode

Transport mode is the default mode for IPSec. It is used for end-to-end security between a client and a server within a LAN. IPSec can encrypt the payload of each packet to protect the integrity and confidentiality of the data that it contains. As an alternative, IPSec can simply be used to ensure that the communication came from the indicated source and that the communication hasn’t been intercepted or tampered with while in transit. Based on your own security needs, you can configure IPSec for one of the following:

➤ Authentication Header (AH) transport mode
➤ Encapsulating Security Payload (ESP) transport mode

Authentication Header (AH) Transport Mode

Authentication Header (AH) provides for authentication, integrity, and anti-replay of each packet without encrypting the data. In other words, the data remains readable but is protected from modification. AH uses a system of keyed hash algorithms to sign the packet to ensure its integrity. In this way, you can be assured that a packet did originate from its indicated source and that it has not been modified in transit. This is accomplished by placing an AH header in each packet between the IP header and the IP payload. You can configure custom data integrity and encryption settings, as illustrated on Figure 3.8. Configuring custom settings requires the following steps:

1. Locate or create an IPSec policy in a computer’s Local Settings, a domain’s Default Security Policy, or a Group Policy Object.
2. Right-click the IPSec policy.
3. Click Properties.
4. Select the Default Response rule.
5. Click Edit.
7. Select Custom.
8. Click Settings.

AH does not encrypt the data within the packets sent.
Figure 3.8 IPSec can be used to protect the integrity of a packet using AH.

**Encapsulating Security Payload (ESP) Transport Mode**

*Encapsulating Security Payload (ESP)* provides everything that AH does and also provides for the confidentiality of the packet during transit. In transport mode, the entire packet is not encrypted or signed; rather, only the data in the IP payload is encrypted and signed. The authentication process ensures that the packet originated from the indicated sender, and the fact that the data was encrypted ensures that it wasn’t viewed or modified during transit. This is accomplished by placing an ESP header before the IP payload and an ESP trailer after the IP payload, further encapsulating only the IP payload.

![ESP does not sign the entire packet—only the IP payload itself is encrypted.](image)

**Tunnel Mode**

IPSec tunnel mode encrypts the IP header and the payload during transit. In this way, tunnel mode provides protection for the entire packet. An entire IP packet is first encapsulated with an AH or ESP header, and then the result is encapsulated with an additional IP header. The additional IP header contains the source and destination of the tunnel endpoints. After the packet reaches the first destination at the tunnel endpoint, it can be decapsulated and sent to the final destination by reading the IP address.
This double encapsulation makes tunnel mode suitable for protecting traffic between network systems. It can be used when traffic must pass through an untrusted medium such as the Internet. It is therefore most often used with gateways or end-systems that do not support L2TP/IPSec or PPTP connections. You can use IPSec tunnel mode for the following configurations:

➤ Gateway to gateway
➤ Server to gateway
➤ Server to server

As with transport mode IPSec, tunnel mode IPSec can be used in AH mode or in ESP mode. The concept is very much the same except that the packets are encapsulated twice. You can configure IPSec tunnel mode for the following:

➤ AH tunnel mode
➤ ESP tunnel mode

**Authentication Header (AH) Tunnel Mode**
AH tunnel mode encapsulates an IP packet by placing an AH header between the internal IP header and the external IP header. AH then signs the entire packet for integrity and authentication. This is illustrated in Figure 3.9.

**Encapsulating Security Payload (ESP) Tunnel Mode**
ESP mode encapsulates an IP packet with an ESP header, IP header, and payload. This has the effect of protecting the IP header, trailer, and payload. The entire packet is then encapsulated into a new IP tunnel header, which contains the IP addresses of the endpoints of the tunnel. This is illustrated in Figure 3.10.

Transport mode IPSec is used for secure communications between client and servers in a LAN, whereas tunnel mode is used for secure communication between networks.
Implementing and Managing Security for Network Communications

**Figure 3.9** In AH tunnel mode, authentication headers are placed between the internal IP header and the external IP header of each packet.

**Figure 3.10** In ESP tunnel mode, the entire packet is encapsulated into a new IP tunnel header, which contains the IP addresses of the endpoints of the tunnel.

**IPSec Policy Rules**

Whether you use transport mode or tunnel mode for IPSec, the behavior of the system will be determined and controlled by the rules that you configure. Windows Server 2003 comes installed with some basic rules, but these are only to be used for examples because they offer no real security for your network. You should configure rules based on the security requirements of your organization. How you configure the rules of a policy will determine how it will be used and ultimately whether it will be in transport mode or tunnel mode.
Each IPSec policy consists of one of more rules that will determine the behavior of the policy. The rules are configured on the Rules tab of the properties of an IPSec policy, as shown in Figure 3.11. You can access the Rules tab by right-clicking a policy and clicking Properties. Each rule can contain settings for the following:

- Filter list
- Filter action
- Authentication methods
- Tunnel endpoint
- Connection type

![Filter List](image)

**Figure 3.11** You can configure the properties of each IPSec rule.

**Filter List**

You configure a filter list by selecting the IP Filter List tab in the properties of an IPSec rule (see Figure 3.12). In the resulting IP Filter List dialog box,
a single filter list can contain multiple predefined packet filters that allow traffic to be identified by the list. After the traffic is identified, then the filter action can be applied. Filter lists can identify traffic based on its source, destination, and protocol. You can set both inbound and outbound filters in an IPSec policy.

Figure 3.12  You can configure multiple filter lists in a single IPSec policy.

Filter Action
A filter action is set for each type of traffic as identified by a filter list. The filter actions from which you can choose include Permit, Block, or Negotiate Security for the packets that match the filter list. If Negotiate Security is selected, one or more security methods can be selected. Filter actions are configured on the Filter Action tab in the properties of an IPSec rule. As mentioned previously, the system automatically processes multiple filters in order of specificity, starting with the most specific.

Authentication Methods
You can configure one of more authentication methods to be used in main mode during negotiations. The available authentication methods (as discussed previously) are Kerberos V5, certificates, and preshared keys. You should only use preshared keys as a last resort. You can configure these using the Authentication Methods tab in the properties of an IPSec rule.

Tunnel Endpoint
When you configure a tunnel endpoint as part of a rule, you are setting up one end of tunnel mode IPSec. You must also configure the other end of the
tunnel with the same rule and its corresponding tunnel endpoint. This establishes the IP addresses that will be used when the packet is encapsulated before being sent through the tunnel. You should configure the tunnel endpoint on the Tunnel Setting tab in the properties of the IPSec rule to which it applies.

Connection Type
The connection type specifies whether this rule applies to LAN communications, dial-up, or both. The connection type setting can be used to specify rules based on the inherent protocols and technologies that your connection uses. In other words, LAN communications will certainly use different protocols (rules) than dial-up communications and will therefore require different IPSec rules as well.

Deploying and Managing IPSec Policies
Using Group Policy, IPSec policies can be set on a single computer, an entire domain, an entire site, or any AD organizational unit (OU). You can create, modify, and deploy IPSec policies using the IP Security Policy Management Console, as shown in Figure 3.13.

Figure 3.13 You can create, modify, and deploy IPSec policies using the IP Security Policy Management console.
You should be familiar with the following aspects of deploying and managing IPSec policies:

- Deploying IPSec using Local Policy objects
- Deploying IPSec using Group Policy objects (GPOs)
- Deploying IPSec using commands and scripts
- Deploying IPSec certificates

**Deploying IPSec Using Local Policy Objects**

You can configure the properties of IPSec and create rules using the Local Security Policy Microsoft Management Console (MMC), as shown in Figure 3.14, on Windows 2000 Professional and all later clients and on member servers. The Local Security policy is located in Administrative Tools. Any policy defined in a Group Policy will override any policy that is deployed only to the local computer. In other words, if the computer is part of an AD, the IPSec policies defined in Group Policy that apply to its container will override its local policy.

![Local Security Settings](image)

**Figure 3.14** You can configure IPSec in the Local Security policy of a client or member server.
Deploying IPSec Using Group Policy Objects

IPSec polices are one of the security settings in each GPO. You can use Group Policy to configure IPSec for an entire domain, an entire site, or selected OUs. Group Policies are processed in the order of local, site, domain, OU, and finally child OU, and any IPSec policies that conflict will be overridden by the next level of processing. In other words, the IPSec policies that will ultimately apply will be only those that are applied to the container in which the object actually resides as well as any policies that did not conflict in the entire processing order. Figure 3.15 shows IPSec settings in a GPO.

![Group Policy Object Editor](image)

**Figure 3.15** You can configure IPSec within GPOs.

Deploying IPSec Using Commands and Scripts

If all of the computers on which you are running IPSec are part of the Windows Server 2003 family, you can deploy IPSec using the `netsh ipsec` command. This method of deployment can be useful when you want to script the IPSec configuration and run the same script on multiple servers. It also provides some advanced fine-tuning for management and security that is not available in the GUI mode.
You can choose from two major types of commands. You make your choice based on whether you are creating a new policy that be immediately effective or creating a policy that will be applied later. The two major types of netsh ipsec commands are as follows:

➤ Netsh ipsec static

➤ Netsh ipsec dynamic

**Netsh ipsec static**
You can use netsh ipsec static commands to create, modify, and assign IPSec policies without immediately affecting the active IPSec policies. This is very much like creating a new policy and new rules within the GUI and not immediately assigning the policy. To view the netsh ipsec static commands, type netsh ipsec static /? at a command prompt.

**Netsh ipsec dynamic**
You can use netsh ipsec dynamic commands to display the active state of IPSec and to immediately affect the configuration of the active IPSec policy. You use dynamic commands to directly configure the security policy database (SPD). To view the available netsh ipsec dynamic commands, type netsh ipsec dynamic /? at a command prompt.

**NOTE**
Most dynamic commands take effect immediately, but some require you to restart the IPSec Policy Agent or restart the computer.

**Deploying IPSec Certificates**
As mentioned previously, IPSec can use one or more of three authentication methods. These include Kerberos V5, preshared keys, and certificates. You can only use Kerberos if all of the computers to be authenticated are part of your AD. You should only use preshared keys if absolutely necessary. This means that certificates should be used the balance of the time.

To be more specific, you should use certificates whenever communications include Internet access, remote access, external business partners, or computers in your network that cannot use the Kerberos V5 protocol. The use of certificates will require at least one certification authority (CA). This authority can be set up in your own hierarchy or can be a commercial CA. You can use the certification authority and Group Policy provided by Windows Server 2003 to automatically enroll certificates for computers on
your network, and computers outside of your network require a third-party
CA (such as VeriSign) and manual account mapping for the certificates used.
Account mapping maps the computer certificate to a particular computer
account, which can be within your organization or another organization.

Microsoft clients and servers prior to Windows 2000 do not use the Kerberos pro-
tocol.
Exam Prep Questions

Question 1

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. AH transport mode
- B. ESP transport mode
- C. ESP tunnel mode
- D. AH tunnel mode

Answer B is correct. ESP transport mode should be used to ensure the integrity and confidentiality of data that is exchanged within the same LAN. AH transport would only ensure the integrity of the LAN data, not the confidentiality; therefore, answer A is incorrect. ESP tunnel mode should be used to secure the integrity and confidentiality of data between networks and not within a network; therefore, answer C is incorrect. AH tunnel mode should be used to secure the integrity of data between networks and not within a network; therefore, answer D is incorrect.

Question 2

Which two types of encryption protocols can be used to secure the authentication of computers using IPSec?

- A. Kerberos V5
- B. Certificates
- C. SHA
- D. MD5

Answers C and D are correct. SHA or MD5 can be used. Kerberos V5 is an authentication protocol, not an encryption protocol; therefore, answer A is incorrect. Certificates are a type of authentication that can be used with IPSec, not an encryption protocol; therefore, answer B is incorrect.
Chapter 3

Question 3

Which type of authentication should a company that has all computers in one domain use to ensure authentication of all clients and servers with the least administrative effort? Assume that all client computers run Windows XP Professional and all servers run Windows Server 2003.

❍ A. Certificates
❍ B. Preshared keys
❍ C. Kerberos V5
❍ D. MD5

Answer C is correct. Kerberos V5 is the default authentication protocol for clients running Windows XP Professional and servers running Windows Server 2003 in a domain environment. Certificates would require much more administrative effort in comparison to Kerberos V5; therefore, answer A is incorrect. Preshared keys should only be used when absolutely necessary; therefore, answer B is incorrect. MD5 is an encryption protocol and not an authentication protocol; therefore, answer D is incorrect.

Question 4

Which two types of IPSec can be used to secure communications between two LANs?

❑ A. AH tunnel mode
❑ B. ESP tunnel mode
❑ C. AH transport mode
❑ D. ESP transport mode

Answers A and B are correct. A tunnel mode IPSec should be used. AH transport mode is for protection of the integrity of data transferred between computers on a LAN; therefore, answer C is incorrect. ESP transport mode protects the integrity and confidentiality of data transferred by computers within a LAN; therefore, answer D is incorrect.
Question 5

Which part of an IPSec policy contains filters and filter actions and controls the behavior of the policy?

- A. Authentication
- B. Encryption
- C. Tunneling
- D. Rules

Answer D is correct. Rules contain filters and filter actions and control the behavior of an IPSec policy. Authentication is the process of proving an identity; therefore, answer A is incorrect. Encryption is the process of scrambling data to protect its confidentiality; therefore, answer B is incorrect. Tunneling is the process of encapsulating one protocol into another; therefore, answer C is incorrect.

Question 6

Which of the following are settings in an IPSec rule? (Choose two.)

- A. Types of operating systems allowed
- B. Filters
- C. Connection types
- D. RAM required

Answers B and C are correct. Parts of an IPSec rule can include filters, filter actions, authentication methods, connection types, and tunnel endpoints. Types of operating systems allowed is not a rule setting; therefore, answer A is incorrect. RAM required is not a rule setting; therefore, answer D is incorrect.

Question 7

Which IPSec rule setting defines traffic that is to be identified?

- A. Filter action
- B. Filter
- C. Tunnel endpoint
- D. Connection type
Answer B is correct. A filter defines traffic that is to be identified. Filter action identifies how traffic will be handled after it is identified; therefore, answer A is incorrect. Tunnel endpoint identifies the predefined IP address of the router of a remote network; therefore, answer C is incorrect. Connection type identifies whether the connection can be LAN, dial-up, or both; therefore, answer D is incorrect.

**Question 8**

Which two components of a rule work together to identify packets and then make decisions that affect traffic flow and security?

- A. Kerberos V5
- B. Filters
- C. Filter actions
- D. Connection types

Answers B and C are correct. Filters and filter actions work together to identify packets and then make decisions that affect traffic flow and security. Kerberos V5 is an authentication protocol that runs by default; therefore, answer A is incorrect. Connection types identify whether a rule applies to a LAN, dial-up, or both; therefore, answer D is incorrect.

**Question 9**

Which AD service should you use to distribute IPSec policies that affect all of the computers in a single domain?

- A. AD replication
- B. Kerberos V5
- C. Group Policy
- D. Remote Installation Services (RIS)

Answer C is correct. You should use Group Policy to distribute IPSec policies that affect all of the computers in a single domain. AD replication is not involved in the distribution of IPSec policies to a domain; therefore, answer A is incorrect. Kerberos V5 is the default authentication protocol for AD, but is not involved in distributing IPSec policies; therefore, answer B is incorrect. You can use RIS to install new clients and servers, but RIS is not involved in distributing IPSec policies; therefore, answer D is incorrect.
Question 10

Which two tools should you use to create, manage, and deploy IPSec policies?

- A. Local Security Policy MMCs for each computer
- B. IP Security Policy Management Console
- C. `netsh ipsec`
- D. Active Directory Sites and Services

Answers B and C are correct. The IP Security Policy Management Console and the `netsh ipsec` command can both be used to create and deploy IPSec policies. Local security policies on each computer cannot be used to control an entire domain; therefore, answer A is incorrect. Active Directory Sites and Services cannot be used to control the IPSec policies for a domain; therefore, answer D is incorrect.