# **Module 11**

**Managing and Securing Windows Networks**

|  |
| --- |
| **At a Glance** |

#### Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

# **Overview**

This module focuses on securing and maintaining a Windows Server 2019 environment. Your students first learn about the Group Policy editor and how it can be used to secure and manage systems and software in a domain environment. The next two sections cover public key certificates and the deployment of systems and software in a domain environment. It is important for students to clearly and thoroughly understand the use and management of digital certificates, as well as the certificate authority process. Plan to spend some time in these two sections to cover the material appropriately. Once this material is understood, students are presented with the knowledge they will need to protect WLAN access using 802.1X Wireless techniques. Finally, the last two sections introduce the concepts of software maintenance using the Windows Server 2019 WSUS component and system software protection using Windows Defender settings, firewall rules, and IPSec. Understanding both of these topics is critical to maintaining a healthy and safe server environment that will host a variety of applications necessary for successful organizational operation. As you end this module, make sure students understand the need for and importance of maintaining a clean server setup.

# **Module Objectives**

* Configure and manage GPOs
* Identify the structure and use of public key certificates
* Deploy certificates using an enterprise CA
* Protect WLAN access using 802.1X Wireless
* Use WSUS to manage the distribution of updates
* Configure Windows Defender settings, firewall rules, and IPSec

# **Teaching Tips**

**Configuring Group Policy**

1. Remind students that Active Directory can provide centralized authentication and single sign-on capability.
2. Point out that Active Directory contains a powerful administrative feature called Group Policy.
3. Review the items Group Policy can automatically configure such as software; Windows features; and security, program, and user interface settings on computers in an Active Directory domain based on the location of a user or computer account in the Active Directory database.
4. Mention that to configure Group Policy, an administrator creates Group Policy Objects (GPOs) that have the appropriate settings.
5. Note that a single GPO can be applied to thousands of users and computers in an organization to reduce the time and effort that it takes to administer a large domain.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | To function, GPOs must be linked to a site, domain, or OU object that contains the user or computer accounts that it applies to. Unlike its name suggests, GPOs do not apply to Active Directory groups. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Be sure to mention that GPO settings are strictly enforced. As a result, users are not able to configure or override settings that are applied by GPOs. |

1. Mention that Group Policy settings are stored in two different sections in a GPO.

* Computer Configuration
* User Configuration

1. Explain when each section in a GPO is applied.
2. Review the order GPOs are applied to user and computer accounts, and explain why this needs to take place.
3. Mention that if multiple GPOs are linked to the same site, domain, or OU, they will be applied in link order, with the highest link order applied first and the lowest link order applied last.
4. Discuss the two default GPOs in each Active Directory domain that provide default security configuration for computers.

* The *Default Domain Policy* GPO is linked to the domain object and applies to all user and computer accounts in the domain.
* The *Default Domain Controllers Policy* GPO is linked to the Domain Controllers OU and applies to domain controller computer accounts.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Mention that for performance reasons, an administrator should only link GPOs to site objects when no alternative options are viable. This is because each client must first match their IP configuration to a subnet that is associated with a site object in order to identify the site of which they are a part. |

**Configuring GPOs**

1. Explain that to configure GPOs in an Active Directory environment an administrator starts the Group Policy Management tool. Discuss how to start this tool.
2. Refer to Figure 11-1 to illustrate the Group Policy Management tool. Review the contents displayed in the figure.
3. Mention that an administrator can configure the Block Inheritance setting on an OU to prevent user and computer accounts in the OU from applying GPOs that are linked to parent OUs, domains, or sites.
4. Mention that an administrator can also configure the Block Inheritance setting on a domain to prevent domain user and computer accounts from applying GPOs that are linked to sites.
5. Emphasize that if a GPO link is configured with the Enforced setting, the associated GPO will be applied to user and computer accounts in domains and OUs that have Block Inheritance configured, and will be applied following other GPOs to ensure that its settings override the same settings in other GPOs.
6. Refer to Figure 11-1 again and note that the blue exclamation point icon on the R&D OU indicates that the Block Inheritance setting has been configured. Note that the yellow lock icon on the Default Domain Policy link to domainX.com indicates that it is Enforced to ensure that the Default Domain Policy GPO applies to all OUs, including the R&D OU.
7. Explain that to block inheritance on a domain or OU object, an administrator can right-click it in the navigation pane and then click Block Inheritance. Explain that in a similar manner, to enforce a GPO link, an administrator can right-click it in the navigation pane and click Enforced.
8. Refer to Figure 11-1 again. Mention that the Default Domain Policy applies to all user and computer accounts in domainX.com because the Authenticated Users group (which contains all authenticated user and computer accounts in the domain) is listed in the Security Filtering section of the Scope tab of Default Domain Policy properties.
9. Describe how to apply the Default Domain Policy GPO to specific users and computers.
10. Remind student that an administrator can use WQL (WMI Query Language) statements to obtain information from Windows systems using WMI.
11. Mention that to further limit the computers that a GPO applies to, an administrator can configure GPOs with a WMI filter that specifies the hardware and software features that must be present on a computer before the GPO is applied.
12. Refer to Figure 11-1 again. Point out the Laptops Only WMI filter in the properties of the Default Domain Policy GPO and note that the GPO applies to laptop computers in the domain only.
13. Describe how to create a Laptops Only WMI filter.
14. Describe how to create a new GPO and then link this GPO to one or more site, domain, or OU objects. Emphasize that after a GPO is linked to a site, domain, or OU object, a link object for the GPO is displayed underneath.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | In addition to supplying a GPO name, an administrator is prompted to optionally select a starter GPO when creating a new GPO. A starter GPO is a template GPO that contains Administrative Templates settings that are automatically applied to the new GPO. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | If an administrator links multiple GPOs to the same site, domain, or OU, he or she can modify the link order for the GPOs. |

**Configuring GPO Settings**

1. Mention that to modify GPO settings, an administrator will need to use the Group Policy Management Editor. Describe how to start this tool.
2. Refer to Figure 11-2 to illustrate the Group Policy Management Editor.
3. Mention that the Computer Configuration and User Configuration sections of each GPO contain two folders.

* *Policies* contains Group Policy settings, organized into three subfolders:
  + Software Settings specifies software packages that are deployed to computers.
  + Windows Settings provides operating system configuration.
  + Administrative Templates provides configuration for desktop and operating system components.
* *Preferences* contains Group Policy preferences. Group Policy preferences can be used to provide configuration for Windows features. Unlike Group Policy settings, Group Policy preference configuration is not strictly enforced and can be modified by users afterward.

1. Emphasize that there are over 5,000 different individual settings available under the folders and subfolders in a GPO.
2. Mention that the Software Settings folder in a GPO allows an administrator to deploy software to computers using Group Policy. Emphasize that this software is typically hosted in a shared folder on a file server and packaged as a Windows Installer file (.msi).
3. Review the three software deployment methods that an administrator can choose.

* Software that is Published under Software Settings in the User Configuration of a GPO can be optionally installed by users.
* Software that is Assigned under Software Settings in the User Configuration of a GPO is made available as a program icon on the Start menu, as well as a file association.
* Software that is Assigned under Software Settings in the Computer Configuration of a GPO is automatically installed the next time the computer is booted.

1. As an example, refer to Figure 11-3 to illustrate how the Mozilla Firefox software package is published under the Software Settings in the User Configuration of the Default Domain Policy GPO.
2. Refer to Figure 11-3 again and explain how to deploy software packages.
3. Mention that Group Policy can be configured to automatically uninstall software when the GPO no longer applies to the user or computer account to which the software was deployed.
4. Review the situations where a GPO will no longer apply to a user or computer account.
5. As an example, refer to Figure 11-3 again and explain how to configure computers to automatically uninstall Mozilla Firefox if the Default Domain Policy GPO no longer applies.
6. Refer to Figure 11-4 and explain that the Windows Settings folder in a GPO contains subfolders that an administrator can use to configure different Windows settings. Review the various subfolders.

* Name Resolution Policy
* Scripts (Startup/Shutdown)
* Scripts (Logon/Logoff)
* Deployed Printers
* Security Settings
* Folder Redirection
* Policy-based QoS

1. Emphasize that the Security Settings subfolder of Windows Settings in the Computer Configuration section is often the focus for server administrators who wish to secure the computers in the domain.
2. As an example, refer to Figure 11-5 and mention that the Account Policies subfolder of Security Settings contains a Password Policy subfolder that holds settings server administrators use to configure password settings. Refer to Table 11-1 for the password policy settings. Review the settings in Table 11-1 and Figure 11-5.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Mention that an administrator can double-click a setting to modify its value or view its description. |

1. As another example, refer to Figure 11-6 and mention that the Account Lockout Policy subfolder of Account Policies allows server administrators to automatically lock user accounts after a certain number of invalid login attempts. Refer to Table 11-2 for the account lockout policy settings. Review the settings in Table 11-2 and Figure 11-6.
2. Mention that most configuration settings in a GPO are stored under the Administrative Templates folder.
3. Refer to Figure 11-7 and mention that this folder contains several subfolders that can be used to configure different Windows components.

* Control Panel
* Desktop
* Network
* Printers
* Server
* Shared Folders
* Start Menu and Taskbar
* System
* Windows Components
* All Settings

1. Mention that each setting under the Administrative Templates folder describes its function, and can be set to Enabled to provide the function, or Disabled to prevent the function if another GPO processed earlier is configured to provide it.
2. As an example, refer to Figure 11-7 again and explain that the Desktop configuration ensures that the Internet Explorer icon is hidden but that the Recycle Bin icon is shown.
3. Mention that the list of folders available under Administrative Templates can be expanded to include additional configuration settings. Note that many third-party software manufacturers allow an administrator to download and install administrative template files that can be imported into a GPO and used to configure settings for their software.
4. Emphasize that administrative templates files for legacy systems end in .adm while administrative templates files for Windows Vista SP1, Windows Server 2008, and newer systems end in .admx and may be accompanied by folders that include language customizations.
5. Refer to Figure 11-8 and review how to import the various template and language files.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | If an administrator edits a starter GPO, Administrative Templates is the only folder available under the Computer Configuration and User Configuration sections. The settings in all other GPO folders cannot be configured in a starter GPO. |

1. Refer to Figure 11-9 and explain how to configuring Group Policy preferences.
2. Mention that the Preferences folder contains two subfolders that include the configurable features.

* Windows Settings allows an administrator to add, remove, or modify applications, drive maps, shared folders, environment variables, files, folder, shortcuts, and registry keys.
* Control Panel Settings allows an administrator to configure users, groups, settings, and devices in Control Panel.

1. Explain that an administrator can use Group Policy preferences to configure some of the same Windows features that are available in the Windows Settings and Administrative Templates folders under the Policies folder in a GPO.
2. Point out that Group Policy preferences allows for additional feature configuration options. Most features configured using Group Policy preferences allow an administrator to specify the configuration action that must be performed.

* Create configures a new feature only if it does not already exist.
* Replace replaces an existing feature configuration with a new one.
* Update modifies a previously configured feature to include new settings.
* Delete removes a feature if it was previously configured.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | After an administrator modifies a setting in the Group Policy Management Editor, that setting is automatically saved to the GPO object in the Active Directory database as well as copied to the associated file in the SYSVOL share, where it can be accessed by domain computers. As a result, there is no Save button available in the Group Policy Management Editor. |

**Managing GPOs**

1. Mention that after an administrator configures a new GPO, the administrator should review its settings to ensure they match the organization’s needs, and document them for future use.
2. Refer to Figure 11-10 and explain how to review the configuration and save a report.
3. Refer to Figure 11-10 again and note that because the Computer Configuration and User Configuration sections of the Default Domain Policy GPO contain configured settings, both sections are listed as Enabled.
4. Explain how to choose to configure settings in only one section in a GPO.
5. Emphasize that in general, it is best to minimize the number of settings that an administrator configures in a GPO to ensure that it is processed quickly by clients and to reduce the risk of GPO corruption.
6. Mention the benefit of backing up the GPOs created. Refer to Figure 11-10 and explain how to back up all GPOs.
7. Discuss what actions an administrator should take, including commands to run, if clients do not receive the configuration that the administrator specified in a GPO.
8. Discuss some of the GPO configuration issues that can prevent clients from applying a GPO and explain how to troubleshoot the issues.
9. Introduce the Group Policy Results Wizard in the Group Policy Management tool and mention that it can be used to troubleshoot the application of Group Policy.
10. Explain how to start the Group Policy Results Wizard.

**Deploying Public Key Certificates**

1. Introduce this section by mentioning that many different technologies rely on the use of public key certificates for the encryption of data.
2. Point out that to support the use of these technologies in an organization, an administrator must understand the function of public key certificates, as well as the process used to deploy them to users and computers in an organization.

**Understanding Public Key Certificates**

1. Remind students that EFS uses both symmetric and asymmetric encryption to protect the contents of files.
2. Describe how encryption works when an administrator encrypts a file using EFS. Mention how most technologies that encrypt data across a network use both symmetric and asymmetric encryption together in a similar way.
3. Refer to Figure 11-11 and review the encryption steps that take place when a user accesses a website using HTTPS.
4. Describe the man-in-the-middle attack security weakness that affects the process shown in Figure 11-11.
5. Explain how to prevent man-in-the-middle attacks by sending public keys to a trusted third-party computer called a Certification Authority (CA) for endorsement before they are used for secure technologies, such as HTTPS. Note that this process is called enrollment.
6. Mention that after the CA verifies the identity of the user or computer that generated the public key, it creates a public key certificate that includes several items. Review and explain each item.

* A serial number
* A certificate name
* Intended certificate uses and technologies (e.g., EFS, HTTPS, IPSec, L2TP, IKEv2, email encryption, secure authentication, and so on)
* A public key
* A digital signature of the public key
* A time period for which the certificate is valid (typically 1 year)
* The location of the Certificate Revocation List (CRL)
* The location of the CA’s public key (called the trusted root)

1. Emphasize that the most important part of a certificate is the digital signature.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | A hash (also called a checksum) is a calculation performed on the contents of a file or set of data. As a result, hashes are often used to determine whether data has been modified in transit. |

1. Explain that after a CA creates a certificate, it returns it to the computer that generated the public key such that it can be used for secure technologies, such as HTTPS.
2. Point out that because the CA only issues certificates and does not directly participate in the encryption process, it maintains a list of any issued certificate serial numbers that should not be used in the CRL. Describe purpose of the CRL.
3. Refer to Figure 11-12 and review the steps of that take place when a user accesses a website using HTTPS using a public key certificate to protect HTTPS.
4. Review the many technologies in an organization that use certificates for secure access. Be sure to mention Web servers and Web apps (using HTTPS), IPSec, VPNs (SSTP, L2TP, IKEv2), DirectAccess, IPP (using HTTPS), EAP authentication, and EFS.
5. Note that some technologies do not require certificates to function, but will use them to prevent man-in-the-middle attacks if available.
6. Mention that to provide secure access to technologies that support certificates, an administrator must provide the associated certificates for the users and computers in the organization.
7. Explain the role of public CAs in terms of providing certificates to users. Explain how to obtain a certificate from a public CA.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Public CAs are also called commercial CAs. |

1. Introduce the concept of an enterprise CA. Note that obtaining certificates from a public CA for each user and computer in an organization is impractical. Therefore, an administrator can instead configure a Windows Server 2019 system as an enterprise CA in the organization that can be used to issue certificates automatically to users and computers using certificate templates and Group Policy.
2. Mention that this process is called auto-enrollment and simplifies the management of certificates in an organization. Point out that because the trusted root of an enterprise CA is normally provided to organization computers only, only users and computers in the organization can validate certificates that were issued by an enterprise CA.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | When auto-enrollment is configured, the trusted root of an enterprise CA is automatically distributed to each domain computer using Group Policy. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Organizations that use an enterprise CA to issue certificates to their users and computers are said to have a public key infrastructure (PKI). |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Large organizations can have several CAs configured in a CA hierarchy. The first CA deployed in a hierarchy is called the root CA and other CAs that participate in the hierarchy are called subordinate CAs. In most organizations, only a single enterprise root CA is necessary. |

**Installing an Enterprise CA**

1. Emphasize that to configure Windows Server 2019 as an enterprise CA, an administrator must first install the Active Directory Certificate Services server role.
2. Refer to Figure 11-13. Explain that when an administrator selects the Active Directory Certificate Services server role in the Add Roles and Features Wizard and progresses through the wizard, the administrator is prompted to choose the role services to install. Review all of the role services.
3. Explain that after the necessary role services have been installed, an administrator can click *Configure Active Directory Certificate Services* *on the destination server* on the final page of the Add Roles and Features Wizard to open the AD CS Configuration wizard.
4. Mention that the default selections shown by this wizard configure an enterprise root CA called domain-server-CA that contains a new 2048-bit public/private key pair, and uses the SHA-256 algorithm to hash public keys when generating digital signatures for certificates. Emphasize that these settings are appropriate for most environments.

**Configuring an Enterprise CA for Certificate Enrollment**

1. Refer to Figure 11-14 and explain that after an administrator has installed an enterprise CA on a Windows Server 2019 system, he or she can configure it using the Certification Authority tool. Explain how to open this tool.
2. Mention that the folders under the domainX-SERVERX-CA server object in Figure 11-14 are used to manage and configure most CA functionality. Review the folders.

* Revoked Certificates
* Issued Certificates
* Pending Requests
* Failed Requests
* Certificate Templates

1. Mention that before users and computers in a domain can obtain certificates, the administrator must configure certificate templates that contain the appropriate settings and permissions. Explain how to open the Certificate Templates Console where this configuration can take place.
2. Refer to Figure 11-15 to illustrate the Certificate Templates Console.
3. Mention that each certificate template available in the Certificate Templates Console contains settings that the CA can use to issue certificates for a particular use or technology. Provide some examples.
4. Refer to Figure 11-15 and mention that the number in the Schema Version column reflects the minimum computer version that can use the template.
5. As an example, refer to Figure 11-16. Mention that to create a schema version 2 copy of the user certificate template in Figure 11-15, an administrator can right-click it, click Duplicate Template, and then specify the appropriate template display name on the General tab, as shown for DomainX User Certificate in Figure 11-16 (spaces are removed to generate the actual template name).
6. Emphasize that the configuration shown in Figure 11-16 ensures that certificates issued using the template are published in Active Directory for quick access by applications and are valid for 1 year. Moreover, certificates that are auto-enrolled using this template are automatically renewed 6 weeks prior to the end of the validity period.
7. Refer to Figure 11-17 and mention that if an administrator highlights the Subject Name tab in Figure 11-16, he or she can specify the information and format used when generating names for certificates that are issued using the certificate template. Review the contents of Figure 11-17.
8. Refer to Figure 11-18. Point out that after configuring the options on the General and Subject Name tabs, an administrator should configure the certificate template permissions on the Security tab. Explain how to manually enroll for a certificate based on a certificate template. Explain how to autoenroll permissions to the certificate template.
9. Refer to Figure 11-18 again. Review and explain the other tabs.

* Issuance Requirements
* Compatibility
* Request Handling
* Cryptography
* Key Attestation
* Superseded Templates
* Extensions
* Server

1. Mention that after an administrator has configured the appropriate certificate template options, he or she can click OK in Figure 11-18 to create the DomainX User Certificate.
2. Note that to allow the DomainX User Certificate to be used by the CA, an administrator must add it to the Certificate Templates folder in the Certification Authority tool.

**Enrolling for Certificates**

1. Mention that the method that an administrator uses to deploy certificates in an organization using an enterprise CA depends on the number of users or computers that require certificates.
2. Note that to configure auto-enrollment, an administrator must first ensure the appropriate certificate templates have been configured to allow Read, Enroll, and Autoenroll permissions to users or computers in an organization. Mention that the next step has an administrator enabling auto-enrollment settings in a GPO that applies to the associated user and computer accounts.
3. Refer to Figure 11-19 and Figure 11-20. Explain how to enable auto-enrollment for user certificates in a GPO.
4. Point out that when a user applies a GPO that has auto-enrollment configured, a public/private key pair is generated in the user account for each new certificate template that grants the user Read, Enroll, and Autoenroll permissions.
5. Note that the public key from each public/private key pair is then sent to the CA for digital signing and returned to the user account as a certificate.
6. Explain that when a computer applies a GPO that has auto-enrollment configured, a public/private key pair is generated in the Windows Registry on the computer for each new certificate template that grants the computer Read, Enroll, and Autoenroll permissions.
7. Point out that the public key from each public/private key pair is then sent to the CA for digital signing and returned to the Windows Registry on the computer as a certificate.
8. Refer to Figure 11-21 through Figure 11-23. Explain how to manually enroll for a user certificate from an enterprise CA.
9. Mention that the process an administrator uses to manually enroll for a computer certificate from an enterprise CA is nearly identical to that used to enroll for a user certificate. Review the process and point out the differences.
10. Remind students that an administrator can use IIS Manager to enroll a computer for an HTTPS certificate.
11. Note that to enroll for an HTTPS certificate from an enterprise CA, an administrator must first configure an appropriate certificate template that grants a computer account Read and Enroll permission.
12. Refer to Figure 11-24. Explain how an administrator can navigate to the Server Certificates feature in IIS Manager, click Create Domain Certificate from the Actions pane, and specify the appropriate information in the Create Certificate wizard.
13. Refer to Figure 11-25. Explain that an administrator must select the enterprise CA and supply a friendly name for the certificate that will be displayed alongside the certificate in IIS Manager. Mention that when an administrator clicks Finish in Figure 11-25, a public/private key pair will be generated in the Windows Registry on the local computer.
14. Note that the public key is then sent to the CA, where it is digitally signed and returned to the Windows Registry on a local computer as a certificate.
15. Point out that this certificate will also be listed in the Server Certificates feature in IIS Manager.

**Quick Quiz 1**

1. True or False: Group Policy Objects (GPOs) apply to Active Directory groups.

Answer: False

1. GPO administrative template files for Windows Vista SP1, Windows Server 2008, and newer systems end in \_\_\_\_\_\_\_\_\_\_.
   1. .win
   2. .new
   3. .adm
   4. .admx

Answer: d. .admx

1. The most important part of a certificate is the \_\_\_\_\_\_\_\_\_\_.
   1. hash
   2. trusted root
   3. digital signature
   4. Certificate Revocation List (CRL)

Answer: c. digital signature

1. Public CAs are also called \_\_\_\_\_\_\_\_\_\_.
   1. commercial CAs
   2. common CAs
   3. enterprise CAs
   4. intermediate CAs

Answer: a. commercial CAs

**Implementing 802.1X Wireless**

1. Open this topic by emphasizing that many users today use mobile devices, such as smartphones and laptops, to access organization resources by connecting to a wireless LAN (WLAN) that relays traffic to a physical LAN in the organization.
2. Note that each WLAN consists of one or more wireless access points (WAPs) that allow mobile devices to connect using Wi-Fi.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | WAPs that are configured to provide a separate IP network for mobile clients are called wireless routers as they must route traffic from the WLAN to the physical LAN. Most small office or home office WAPs are configured as wireless routers by default. |

1. Define and describe WPA.
2. Define and describe WPA2.
3. Define and describe 802.1X Wireless technology. Emphasize that it involves using a RADIUS server to randomly generate symmetric encryption keys for each mobile client. Note that it prevents wireless cracking tools from decrypting WLAN traffic.
4. Refer to Figure 11-26. Explain the steps that take place when a mobile device user connects to a WAP that is configured to use 802.1X Wireless.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Wi-Fi Protected Access III (WPA3) is a recent technology that is supported by some WAPs. While WPA3 does not use a Wi-Fi password in the same way that WPA2 does, it can still be compromised by wireless cracking tools. As a result, organizations also use 802.1X Wireless to protect WPA3 WLANs. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Most organizations implement a separate WLAN for guest access that does not use 802.1X Wireless. This WLAN is configured to allow access to Internet resources only, and not organization resources. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | While less common, 802.1X can also be used to protect access to Ethernet network switches that support it. This technology is called 802.1X Wired. |

**Configuring RADIUS for 802.1X Wireless**

1. Emphasize that to configure a Windows Server 2019 system as a RADIUS server for use with 802.1X Wireless, an administrator must first configure the Network Policy and Access Services server role.
2. Mention that after this server role has been installed, an administrator must use the Network Policy Server tool to activate the server in Active Directory, and create RADIUS clients for each WAP in the organization, noting the shared secret that an administrator configures for each one.
3. Explain that once the server is activated in Active Directory, an administrator must open the Certification Authority tool on his or her enterprise CA and add the *RAS and IAS Server* certificate template to the Certificate Templates folder. Discuss what the certificate template does.
4. Mention that after this certificate template has been added to the enterprise CA, an administrator must use the Certificates MMC snap-in on the RADIUS server to manually enroll for a certificate using it.
5. Refer to Figure 11-27 and explain that after the certificate is manually enrolled, an administrator can highlight NPS (Local) in the Network Policy Server tool, select *RADIUS server for 802.1X Wireless and Wired Connections* and click *Configure 802.1X* to start the Configure 802.1X wizard.
6. Review the available options in Figure 11-27.
7. Refer to Figure 11-28, which illustrates a list of the RADIUS clients that an administrator has previously configured on the RADIUS server. Explain how an administrator can add additional RADIUS clients at this page, and edit or remove existing RADIUS clients.
8. Note that because the network policy for 802.1X Wireless will only apply to WAP RADIUS clients, it is safe to leave existing VPN RADIUS clients in this list.
9. Explain that after an administrator configures the appropriate RADIUS clients in Figure 11-28 and clicks Next, he or she must choose the EAP authentication method.
10. Refer to Figure 11-29 and point out that the Protected Extensible Authentication Protocol (PEAP) method is selected and is required by most WAPs for use with 802.1X Wireless.
11. Explain how an administrator can view the certificate used for PEAP. Point out that if no certificate is shown, an administrator must enroll the RADIUS server for a certificate that uses the *RAS and IAS Server* certificate template.
12. Refer to Figure 11-30 and explain how an administrator specifies the user groups that are allowed to authenticate to the RADIUS server using 802.1X Wireless.
13. Explain that when an administrator clicks Next in Figure 11-30, he or she can optionally specify RADIUS attributes before clicking Next and Finish to complete the configuration.

**Configuring a WAP for 802.1X Wireless**

1. Introduce this topic by mentioning that after an administrator has configured a RADIUS server for 802.1X Wireless, he or she must configure each WAP to use forward authentication requests to the FQDN or IP address of the RADIUS server on port 1812 using the shared secret configured in the associated WAP RADIUS client.
2. Mention that an administrator would do this by accessing the configuration tool for the WAPs in the organization.
3. Explain why an administrator must consult the vendor documentation for the process used to configure 802.1X Wireless for the vendor device.
4. Refer to Figure 11-31 and explain that most WAPs identify 802.1X Wireless using the word “RADIUS” or “Enterprise” in their configuration tool.

**Configuring Windows Server Update Services**

1. Define and describe an update.
2. Introduce the Microsoft Update tool.
3. Mention that the Windows Update section of Control Panel or Settings (Windows 10, Windows Server 2016, and later) is used to search for and install these updates, or schedule automatic update installation.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Windows computers contact the Microsoft Update servers on the Internet using HTTPS (TCP port 443), which is allowed on firewalls by default. |

1. Review some of the problems an organization can experience when obtaining updates from Microsoft Update.

* If several computers in an organization obtain updates from Microsoft Update at the same time, the bandwidth on the organization’s Internet connection could become saturated, preventing access to Microsoft Update and other Internet resources.
* An administrator cannot easily identify computers that have installed a particular update, or prevent the installation of updates that cause problems with other software applications.

1. Explain how an administrator can resolve these problems by implementing a Windows Server Update Services (WSUS) server in the organization.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Computers that are configured to obtain updates from a WSUS server use HTTP on TCP port 8530, or HTTPS on TCP port 8531. |

**Installing WSUS**

1. Emphasize that to configure Windows Server 2019 as a WSUS server, an administrator must first install the Windows Server Update Services server role.
2. Refer to Figure 11-32 and Figure 11-33. Explain the prompts that appear when an administrator selects the Windows Server Update Services server role in the Add Roles and Features Wizard and progresses through the wizard.

**Configuring WSUS**

1. Mention that after an administrator has installed the necessary WSUS role services, he or she can click Windows Server Update Services from the Tools menu in Server Manager to start the Windows Server Updates Services Configuration Wizard.
2. Refer to Figure 11-34 through Figure 11-40. Explain the prompts that appear in the wizard for configuring WSUS.
3. Note that Figure 11-40 illustrates the Update Services tool and an administrator can access the different features under the server in the navigation pane of the tool.

* Updates
* Computers
* Downstream Servers
* Synchronizations
* Reports
* Options

1. Mention that in some organizations, server administrators install new updates on a single computer in each department to ensure that they do not cause problems before they are approved for installation on a WSUS server.
2. Point out that problems caused by updates are rare today and can be easily solved by removing the update. Explain that as a result, many server administrators configure WSUS to automatically approve updates.
3. Refer to Figure 11-41 and explain how to configure WSUS to automatically approve updates.

**Configuring a WSUS GPO**

1. Introduce this topic by mentioning that to ensure computers in an organization obtain updates from the WSUS server instead of Microsoft Update, an administrator must edit the settings of a GPO that applies to the associated computer accounts.
2. Refer to Figure 11-42 and explain how to edit the settings of a GPO.
3. Refer to Figure 11-43 to illustrate how to ensure that these updates are installed from a WSUS server instead of Microsoft Update.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Because modern PCs automatically enter power saving mode when not in use, most organizations require that users leave their computer powered on at the end of the day. This allows GPOs to provide for the automatic installation of updates and other software after working hours. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | If the WSUS server has an HTTPS certificate issued by an enterprise CA, an administrator can specify https in place of http, and 8531 in place of 8530 in Figure 11-43. |

**Configuring Windows Defender**

1. Introduce this section by mentioning that in Windows Server 2019, Windows Defender is started by default and provides many different operating system security features, including malware protection, as well as firewall and IPSec functionality.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Windows Defender has been renamed to Microsoft Defender starting with Windows 10 build 1909. Because Windows Server 2019 still uses the term Windows Defender in configuration tools at the time of this writing, we will refer to it as such in this section. |

**Configuring Windows Defender Features**

1. Explain that if an administrator navigates to Start, Settings, Windows Defender settings and then clicks Open Windows Security, he or she can configure the four main features provided by Windows Defender.
2. Refer to Figure 11-44 to illustrate the four main features provided by Windows Defender. Review and explain each feature.

* Virus & threat protection
* Firewall & network protection
* App & browser control
* Device security

**Configuring Windows Defender Firewall with Advanced Security**

1. Introduce this topic by mentioning that when an administrator installs and configures roles or features in Windows Server 2019, Windows Defender automatically adds a firewall rule to allow inbound and outbound access to the associated programs.
2. Emphasize that most third-party software automatically configures Windows Defender firewall rules to provide for inbound and outbound access to the associated programs. Note that some third-party software requires that an administrator manually add or modify existing firewall rules to provide program access.
3. Refer to Figure 11-45 to illustrate the Windows Defender Firewall with Advanced Security tool. Explain how it is used to manage firewall rules.
4. Refer to Figure 11-46 to illustrate the New Inbound Rule Wizard.
5. Refer to Figure 11-46 through Figure 11-54 and explain how to configure a new firewall rule, configure connection security rules to automatically encrypt IP traffic on the network using IPSec, select the authentication requirements, specify the firewall profiles that should apply the connection security rule, specify a name for the new connection security rule, and create it.
6. Explain how to view active connection security rules.

**Quick Quiz 2**

1. Which technology involves the use a RADIUS server to randomly generate symmetric encryption keys for each mobile client?
   1. WPA
   2. WPA2
   3. WPA3
   4. 802.1X Wireless

Answer: d. 802.1X Wireless

1. When flaws and security weaknesses are discovered in operating systems and other software products, the software vendor releases an associated software \_\_\_\_\_\_\_\_\_\_ to remedy the issue.
   1. update
   2. download
   3. subroutine
   4. module

Answer: a. update

1. Which port do Windows computers use to contact the Microsoft Update servers on the Internet using HTTPS?
   1. UDP port 80
   2. UDP port 443
   3. TCP port 80
   4. TCP port 443

Answer: d. TCP port 443

1. True or False: In Windows Server 2019, Windows Defender is started by default.

Answer: True

# **Class Discussion Topics**

1. When would you use a starter GPO?
2. What is the difference between a digital certificate and digital signature?
3. Why are man-in-the-middle attacks dangerous?

# **Additional Projects**

1. Ask your students to research the Windows Defender product and write a report describing its history and current features.
2. Ask your students to read the following article regarding man-in-the-middle attacks: <https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html>. Then have them write a short report summarizing the dangers of this type of attack and how to prevent it.

# **Additional Resources**

1. Plan your WSUS deployment

<https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/plan/plan-your-wsus-deployment>

1. Microsoft Defender Antivirus on Windows Server 2016 and 2019

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/microsoft-defender-antivirus-on-windows-server-2016>

1. 802.1X Overview and EAP Types

<https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless-networking.html>

1. How Encryption Works: Public Key Encryption

<https://computer.howstuffworks.com/encryption3.htm>

1. What is WPA3?

<https://www.networkworld.com/article/3316567/what-is-wpa3-wi-fi-security-protocol-strengthens-connections.html>

1. Wi-Fi Alliance WPA3 Specification Version 2.0 - PDF (12 Pages)

<https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v2.0.pdf>

1. Designing a CA Hierarchy

<https://docs.aws.amazon.com/acm-pca/latest/userguide/ca-hierarchy.html>

1. The Basics of Cryptography and Digital Certificates

<https://whatismyipaddress.com/cryptography>

**Key Terms**

* **802.1X Wired** 802.1X technology that is used to protect access to Ethernet network switches that support it.
* **802.1X Wireless** Technology where a RADIUS server is used to randomly generate symmetric encryption keys for each mobile client.
* **Active Directory Certificate Services** The server role that allows you to build a public key infrastructure (PKI) and provide public key cryptography, digital certificates, and digital signature capabilities for an organization.
* **administrative template file** Template file that is used by Group Policies to describe where registry-based policy settings are stored in the registry.
* **auto-enrollment** The process of configuring a Windows Server 2019 system as an enterprise CA in your organization that can be used to issue certificates automatically to users and computers using certificate templates and Group Policy.
* **CA hierarchy** A hierarchy that typically has a root CA at the top level under which you have one or more intermediate CAs. (Intermediate CAs are also referred to as policy or subordinate CAs.) Beneath each intermediate CA is one or more issuing CAs.
* **certificate** Short for public key certificate. A system of processes, technologies, and policies that allows you to encrypt and sign data. You can issue digital certificates that authenticate the identity of users, devices, or services.
* **Certificate Revocation List (CRL)** A list of digital certificates that have been revoked by the issuing certificate authority before their scheduled expiration date and should no longer be trusted.
* **certificate template** A certificate template defines the policies and rules that a CA uses when a request for a certificate is received.
* **Certificate Templates Console** Microsoft tool used to manage certificates and configure certificate templates.
* **Certification Authority (CA)** An entity that issues digital certificates.
* **Certification Authority tool** A Microsoft tool used to manage an enterprise CA on a Windows Server 2019 system.
* **checksum** A digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data.
* **commercial CA** Another name for a public CA.
* **connection security rule** Rule that automatically encrypts IP traffic on the network using IPSec.
* **controlled folder access** Controlled folder access is a feature that helps protect your documents and files from modification by suspicious or malicious apps. Controlled folder access is supported on Windows Server 2019 as well as Windows 10 clients. It is especially useful in helping to protect your documents and information from ransomware that can attempt to encrypt your files and hold them hostage.
* **core isolation** A Windows security feature that provides added protection against malware and other attacks by isolating computer processes from your operating system and device.
* **digital signature** A process that guarantees that the contents of a message have not been altered in transit. When you, the server, digitally sign a document, you add a one-way hash (encryption) of the message content using your public and private key pair.
* **enrollment** A process that sends public keys to a trusted third-party computer called a Certification Authority (CA) for endorsement before they are used for secure technologies, such as HTTPS. The process is generally performed immediately after a public/private key pair has been generated.
* **enterprise CA** A Windows Server 2019 system used to issue certificates automatically to users and computers using certificate templates and Group Policy.
* **firewall profile** A firewall profile is a way of grouping settings, such as firewall rules and connection security rules that are applied to the computer depending on where the computer is connected.
* **firewall rule** Firewall rules control how the firewall protects your computer from malicious programs and unauthorized access.
* **Group Policy Management** A way to configure GPOs and provide organizational security.
* **Group Policy Management Editor** A built-in Windows administration tool that enables administrators to manage Group Policy in an Active Directory forest and obtain data for troubleshooting Group Policy.
* **Group Policy Object (GPO)** A collection of settings systems administrators create with the Microsoft Management Console (MMC) Group Policy Editor. The GPO can be associated with one or more of the Active Directory containers, such as sites, domains, or organizational units (OUs).
* **Group Policy preferences** A collection of Group Policy client-side extensions that deliver preference settings to domain-joined computers running Microsoft Windows desktop and server operating systems. Preference settings are administrative configuration choices deployed to desktops and servers.
* **Group Policy Results Wizard** A Microsoft tool that can provide valuable insight into Group Policy processing and application problems.
* **hash** The transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. The digital signature in a certificate is a hash of the public key that is encrypted using the private key of the CA.
* **man-in-the-middle attack** An attack that occurs when an attacker intercepts communications between two parties either to secretly eavesdrop or modify traffic traveling between the two. Attackers might use man-in-the-middle attack attacks to steal login credentials or personal information, spy on the victim, or sabotage communications or corrupt data.
* **memory integrity** A feature of Windows that ensures code running in the Windows kernel is securely designed and trustworthy. It uses hardware virtualization and Hyper-V to protect Windows kernel mode processes from the injection and execution of malicious or unverified code.
* **Microsoft Defender** An anti-malware component of Microsoft Windows.
* **Microsoft Update** A Microsoft service for the Windows family of operating systems, which automates downloading and installing Microsoft Windows software updates over the Internet.
* **Online Certificate Status Protocol (OCSP)** An Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on the Internet standards track.
* **Password Settings Object (PSO)** An Active Directory object. This object contains all password settings that you can find in the Default Domain Policy GPO (password history, complexity, length, etc.). A PSO can be applied to users or groups.
* **Protected Extensible Authentication Protocol (PEAP)** A version of EAP, the authentication protocol used in wireless networks and Point-to-Point connections. PEAP is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control.
* **public CA** A third-party entity that issues certificates for a fee after doing the necessary checks on the organization requesting a certificate.
* **public key certificate** A system of processes, technologies, and policies that allows you to encrypt and sign data. You can issue digital certificates that authenticate the identity of users, devices, or services. See *certificate*.
* **public key infrastructure (PKI)** A set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
* **root CA** The topmost Certificate Authority (CA) in a Certificate Authority (CA) hierarchy.
* **subordinate CA** One of the CAs that lives between the root and end entity certificates. Their main purpose is to define and authorize the types of certificates that can be requested from the root CA.
* **starter GPO** A GPO used to configure settings held under Administrative Templates.
* **synchronization** The process of regularly downloading updates from Microsoft Update for each software product that you have in your organization, as well as distributing them to the computers in your organization.
* **trusted root** The location of the CA’s public key.
* **update** A piece of software that remedies a problem in an application.
* **Update Services tool** A Microsoft tool that assists IT administrators in the effective management of the download and distribution of updates, patches, and hot-fixes released for Microsoft software products to Windows Server operating systems in their network through the use of automation and continuous analyses.
* **Wi-Fi Protected Access (WPA)** The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA. The WPA protocol implements much of the IEEE 802.11i standard.
* **Wi-Fi Protected Access II (WPA2)** WPA2 replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it includes mandatory support for CCMP, an AES-based encryption mode. Certification began in September 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark.
* **Wi-Fi Protected Access III (WPA3)** A replacement for WPA2. The new standard uses an equivalent 192-bit cryptographic strength in WPA3-Enterprise mode, and still mandates the use of CCMP-128 as the minimum encryption algorithm in WPA3-personal mode. The WPA3 standard also replaces the Pre-Shared Key exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016, resulting in a more secure initial key exchange in personal mode and forward secrecy. The Wi-Fi Alliance also claims that WPA3 will mitigate security issues posed by weak passwords and simplify the process of setting up devices with no display interface. Protection of management frames as specified in the IEEE 802.11w amendment is also enforced by the WPA3 specifications.
* **Windows Defender** An anti-malware component of Microsoft Windows.
* **Windows Defender Firewall with Advanced Security** An important part of a layered security model. By providing host-based, two-way network traffic filtering for a device, Windows Defender Firewall blocks unauthorized network traffic flowing into or out of the local device.
* **Windows Installer** A software component and application programming interface of Microsoft Windows used for the installation, maintenance, and removal of software.
* **Windows Internal Database (WID)** A database used by Windows Server Update Services (WSUS). It is used to store information about each software update, such as the computers that have successfully installed it.
* **Windows Server Update Services (WSUS)** A tool previously known as Software Update Services. It is a computer program and network service developed by Microsoft Corporation that enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in a corporate environment.
* **Windows Update** A Microsoft service for the Windows family of operating systems, which automates downloading and installing Microsoft Windows software updates over the Internet.
* **wireless access point (WAP)** A networking hardware device that allows other Wi-Fi devices to connect to a wired network. The AP usually connects to a router as a standalone device, but it can also be an integral component of the router itself.
* **wireless LAN (WLAN)** A wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building.
* **wireless router** A device that performs the functions of a router and includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Depending on the manufacturer and model, it can function in a wired local area network, in a wireless-only LAN, or in a mixed wired and wireless network.
* **WMI filter** The WMI filter is a separate object from the GPO in the directory. A WMI filter consists of one or more queries, and if all queries evaluate to true then the GPO linked to the filter will be applied.