**Module 8 – Implementing and managing security**

**Module Overview**

Organizations face numerous security threats to their data and computing infrastructure. Windows 11 has many security features with which to mitigate these threats. It’s important you know how to configure and use Windows 11 security features to help secure your organization’s devices and data.

**Objectives**

After completing this module, you will be able to:

* Manage user and group accounts
* Configure User Account Control
* Implement BitLocker
* Describe Windows 11 security settings and features
* Describe common network security threats and available mitigations

Lesson 1

**Managing user and group accounts**

When a user wants to use their computer, they must sign in using a user account which identifies them. Users can sign in to Windows 11 using local user accounts, Active Directory domain user accounts, Microsoft accounts, and Azure Active Directory (Azure AD) accounts.

When assigning file permissions and configuring user rights, administrators often use group accounts to accelerate the process. Windows 11 has built-in local groups, but can also utilize Active Directory groups in domain-joined scenarios.

It’s therefore important that you understand how to create and administer both user and group accounts in Windows 11.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Create and manage local user accounts.
* Add work or school accounts.
* Create and manage groups.

**Managing local user accounts**

In order to use a Windows 11 computer, you must sign in. To do so, you’ll need a user account.

**Supported user accounts**

Windows 11 supports a number of different types of user accounts. These include:

* **Local user accounts**. These can only be used on the local computer. By default, at least one usable local user account exists, created during installation.
* **Microsoft accounts**. You can add a Microsoft account to your Windows 11 computer. This account usually has a suffix of Hotmail.com or Outlook.com. By signing in using your Microsoft account, you can synchronize your settings from your other devices. You also can access your OneDrive content across those devices, so effectively, you can sync your data.
* **Organizational accounts**. These are Azure Active Directory (Azure AD) accounts and are associated with your organization’s cloud apps and services. For example, if your organization has a Microsoft 365 subscription, you can use your organizational account (sometimes also referred to as a Microsoft 365 account) to access Microsoft 365 services, such as OneDrive, Exchange, Teams, and SharePoint. Using an Azure AD account also enables you to sync your settings between your devices.
* **Active Directory accounts**. If your services are accessible through an on-premises network, chances are, you’ll be signing in to your Windows 11 computer using an AD DS user account. Computers in an Active Directory domain establish a trust relationship with that domain, enabling the integration and use of domain user and group accounts on the local computer.

**Creating a default account**

When you complete interactive setup of your new computer, which is referred to as completing the out-of-box-experience (OOBE), you are prompted to create an account. You can specify:

* A local account.
* A Microsoft account.
* A work or school (organizational) account.
* An Active Directory domain account.

The default depends on the operating system edition you’re using. For example, with Windows 11 Enterprise, the default is to enter the details for your work or school account. To select another option, in OOBE setup, click **Sign-in options** and then select **Domain join instead**. You can then sign in using a local account and complete the domain-join process. After you’ve signed in, you can add additional accounts as needed.

To review the built-in user accounts:

1. Open **Computer Management** and then expand **Local Users and Groups**.
2. Expand **Users** and review the available user accounts.

It’s likely your computer has the following local accounts:

* **Administrator**. Built-in account for administering the computer.
* **DefaultAccount**. A user account managed by the system.
* **Guest**. Built-in account for guest access to the computer.
* **WDAGUtilityAccount**. A user account managed and used by the system for Microsoft Defender Application Guard scenarios.

You should notice that most accounts are disabled and cannot be used until you enable them. This is a security best practice: only enable accounts that you’re using.

**Adding additional local user accounts**

Although you can use the Settings app to add and manage user accounts, unless the accounts you want to add are Microsoft accounts, you should use Computer Management.

1. Open **Computer Management** and then expand **Local Users and Groups**.
2. Select **Users**, right-click **Users**, and then select **New User**.
3. In the **New User** dialog box, enter the following information and then click **Create**:

* User name
* Full name
* Description
* Password and Confirm password
* Configure these options:
* User must change password at next logon
* User cannot change password
* Password never expires
* Account is disabled

1. Click **Close**.

Any enabled users you add through Computer Management are visible in the Settings app:

1. Open **Settings** and select **Accounts**.
2. Click **Family & other users**.

**Adding a work or school account**

If you have an organizational account, for example, to access Microsoft 365 services, you can add the account to your local Windows 11 computer. What you’re actually doing is adding an Azure AD account on your local computer.

For Windows 11, there are two options for adding an Azure AD account:

* **Azure AD join**. Choose this option for corporately owned devices. It gives your users the best sign-in experience as they use the specified account to sign-in to their computer. This is bit like signing in using an on-premises domain account for an AD DS domain-joined computer.
* **Azure AD register**. Choose this option for personally owned devices. Users do not sign in using the specified account. Instead, they sign in using a local account, and then associate installed apps with the registered account. This is the default.

To add a work or school account using the Azure AD join method, use the following procedure:

1. Open **Settings** and click **Accounts**.
2. Click **Access work or school**.
3. On the **Access work or school** page, click **Connect**.
4. In the Microsoft account dialog box, you have three options:

* **Email address**. Entering the account details performs the action of registering the device with Azure AD and adding the specified user account as a local user.
* **Join this device to Azure Active Directory**. This is the preferred option. It joins the device to Azure AD and enables the user to sign in to their computer with the designated account.
* **Join this device to a local Active Directory domain**. Use this option for joining the device to an on-premises AD DS domain. Note that the computer’s IP settings must enable it to locate domain controllers for the specified domain.

1. Assuming you select **Join this device to Azure Active Directory**, in the **Microsoft account** dialog box, enter the work or school account and click **Next**.
2. Enter the password and click **Sign in**. Depending on organizational security settings, you might be prompted to use a secondary authentication method. For example, entering a code received via text message, or using the Microsoft Authenticator app to confirm the join action.
3. When the **Make sure this is your organization**dialog box displays, click **Join**.
4. When prompted, click **Done**.
5. Restart the computer and then sign in using the organizational account by clicking **Other user**, and then entering the account details.

**Managing groups**

We discussed the benefits of using groups to manage permissions earlier in the course. But you can use groups to perform other administrative tasks, too. For example, you can assign management abilities (rights) to groups. Members of those groups can then perform those management abilities.

On a Windows 11 computer, there are around 20 default groups than you can review using Computer Management. The following table describes some of the more useful groups.

|  |  |
| --- | --- |
| Group | Description |
| Administrators | Have complete and unrestricted access to the computer. |
| Backup Operators | Can override security restrictions for the purpose of backing up or restoring files. |
| Event Log Readers | Can read event logs from local machine. |
| Guests | Have the same access as members of the Users group by default, except for the Guest account which is further restricted. |
| Power Users | Possess limited administrative powers. |
| Remote Desktop Users | Are able to sign in remotely using RDP. |
| Users | Prevented from making accidental or intentional system-wide changes but can run most apps. |

In addition to these groups, Windows also provides a number of *special identities*. These identities behave much like groups (in that you can assign permissions to them, or grant them administrative rights), but they don’t have a membership list. Consequently, you cannot review them in Computer Management.

The following table describes the most important of these special identities.

|  |  |
| --- | --- |
| Special identity | Description |
| Anonymous Logon | Represents connections to a computer and its resources that don’t require authentication. |
| Authenticated Users | Represents authenticated identities. Doesn’t include the Guest account, even if Guest has a password. |
| Everyone | Includes Authenticated Users and the Guest account, unless Guest is disabled. |
| Creator Owner | Represents the security principal that created an object. The Creator Owner has full control permission on any object. |

Typically, it’s not necessary for you to manage local groups on a Windows workstation. If the computer is Active Directory domain-joined, the local group memberships are modified to include Active Directory Global groups. For example, the local Administrators group on a domain-joined computer automatically contains the Domain Admins group from the domain of which the computer is a member. Likewise, Domain Users is added to the local Users group. This approach makes it simple for the computer to be managed by domain administrative accounts, and accessed by domain user accounts.

**Demonstration: Managing accounts**

Lesson 2

**Configuring User Account Control**

With Windows XP and earlier, most users signed in on their computers using an administrative account. This meant that if malicious software was present on the computer, it could execute within an administrative context.

Microsoft introduced User Account Control (UAC) with Windows Vista. UAC enables you to restrict the capabilities of all accounts to those of standard users until it’s necessary for the account to elevate.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe User Account Control.
* Configure User Account Control.

**What is UAC?**

With UAC, even if a user continues to sign in using an administrative account, the account’s capabilities are restricted to those of a standard user. If and when the user performs a task requiring elevation, the user is prompted to confirm that elevation.

This means that if malicious code is attempting to make undesirable system changes, UAC recognizes the attempted use of administrative privilege, and prompts the user. This brings the undesirable system changes to the attention of the user.

The nature of the prompt that you receive depends on whether you’re signed in using a standard user account or an administrator account:

* **Prompt for credentials**. By default, standard users are prompted to confirm the required elevation by entering credentials of an administrator account.
* **Prompt for consent**. Administrator users merely need to confirm the elevation.

When UAC was first introduced in Windows Vista, it was too intrusive, constantly prompting users. Windows 11 generates far fewer prompts, by default. For example, the following actions generate no UAC prompt for standard users:

* Installing updates or drivers from Windows Update.
* Installing drivers included in the driver store.
* Reviewing Windows settings.
* Pairing Bluetooth devices.
* Resetting the network adapter or performing network-diagnostic or network repair tasks.

But the following list contains details about some of the tasks that do require elevation:

* Installing or uninstalling apps.
* Installing a driver for a device where the driver is not in the driver store.
* Configuring Microsoft Defender Firewall.
* Modifying UAC settings.
* Adding or removing user accounts.
* Scheduling Automated Tasks.
* Restoring system backup files.
* Configuring Automatic Updates settings.

**Configuring UAC**

You can configure UAC using Control Panel. The following table describes the available options.

|  |  |
| --- | --- |
| Prompt | Description |
| Never notify me | This turns off UAC. |
| Notify me only when applications try to make changes to my computer (do not dim my desktop) | UAC prompts the user when changes are being attempted that require elevation, but doesn’t dim the desktop. |
| Notify me only when applications try to make changes to my computer (default) | UAC prompts the user when changes are being attempted that require elevation, and dims the desktop. |
| Always notify me | UAC always prompts the user when changes are made to the computer. |

Only an administrator can make these changes.

You can also configure UAC settings by using Group Policy or by using Intune. To use Group Policy, open the Group Policy Management Editor, and navigate to: **Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Security Options**.

The following table describes some of these UAC Group Policy settings.

|  |  |
| --- | --- |
| Policy | Description |
| User Account Control: Admin Approval Mode for the Built-in Administrator account | Controls the behavior of Admin Approval Mode for the built-in Administrator account. If disabled, the built-in administrator runs all tasks with full elevation. |
| User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode | Controls the prompt admin users receive. Options are: Elevate without prompting, Prompt for credentials on the secure desktop, Prompt for consent on the secure desktop, Prompt for credentials, Prompt for consent, Prompt for consent for non-Windows binaries (Default). |
| User Account Control: Behavior of the elevation prompt for standard users | Controls the prompt standard users receive. Options are: Prompt for credentials (Default), Automatically deny elevation requests, Prompt for credentials on the secure desktop. |
| User Account Control: Run all administrators in Admin Approval Mode | Controls UAC. If Disabled, then UAC is disabled. If Enabled, then Admin Approval Mode is enabled. Caution: Don’t disable this setting unless you want to turn off UAC for all users. |

**Demonstration: Configuring UAC**

Lesson 3

**Implementing BitLocker**

Data at rest is sometimes at risk. If you lose your computer, or it’s stolen, your data is definitely at risk. By using BitLocker, you can encrypt your hard drive so that even if you lose your device, the content of the hard disk is inaccessible.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe BitLocker.
* Enable BitLocker.
* Describe BitLocker recovery.

**What is BitLocker?**

Most Windows 11 computers are installed with a single disk. This disk is divided into four partitions. These are:

* EFI System Partition
* Microsoft reserved partition
* Boot Partition
* Recovery Partition

BitLocker helps protect your data by encrypting your hard drive; specifically, the boot partition, also referred to as the Windows drive.

You can also encrypt data drives and removable storage.

Your computer’s content is protected by sign in security. So, someone has to know your Windows user name and password to be able to get access to your computer’s content. To help improve sign in security, you can use Windows Hello to enable two-factor authentication. One of the authentication methods can be biometric: finger print or facial recognition, depending on the hardware configuration of your computer.

But if someone has access to your computer, and can’t bypass Windows Hello two-factor authentication, they can instead remove the physical disk in your computer. They can then attach the disk as an external disk on another computer, and gain access to the content. And that’s where BitLocker comes in. The drive cannot be accessed because it’s encrypted.

BitLocker performs two functions critical functions in your computer:

* **Encryption**. BitLocker encrypts all data stored on the Boot volume (and any data volumes you additionally select). This includes:
* Windows operating system files
* Hibernation and paging files
* Apps and the data that those apps use
* **Integrity**. BitLocker uses a Trusted Platform Module (TPM) by default. This component helps to ensure the integrity of early startup components by ensuring that no modifications have been made to the trusted boot path, including the:
* BIOS
* Boot sector
* Boot manager
* After the TPM verifies that there are no changes, it:
* Releases the decryption key to the Windows OS Loader.
* If the TPM detects changes, it:
* Locks any BitLocker-protected volumes

A TPM is a requirement for Windows 11, but was optional in Windows 10.

**Enabling BitLocker**

BitLocker is enabled by default on Windows 11 devices. So, theoretically, you don’t need to do anything. However, it’s still important that you know how to enable and manage BitLocker settings.

**Enabling BitLocker on C drive**

To enable BitLocker on a computer’s Boot volume, use the following procedure:

1. Open **File Explorer**and navigate to **This PC**.
2. Right-click **Local Disk (C:)**, and then click **Turn on BitLocker**. The BitLocker Drive Encryption wizard starts.

* If BitLocker detects bootable media, for example, an inserted memory stick or bootable DVD, it prompts you to remove it, restart your computer, and start again.

1. On the **How do you want to back up your recovery key?** page, choose from:

* Save to your Microsoft account
* Save to a file
* Print the recovery key
* Your options might vary depending on the type of account you are signed in with.

1. Click **Next**, and BitLocker encryption starts.

You are not prompted to choose how to unlock your drive because the default is to use a TPM.

**Enabling BitLocker using Intune**

For organizations that use Microsoft Intune for device management, you can use Intune to enable BitLocker. There are several ways that you can do this, but a common approach is to use a device Configuration profile, and choose a profile type of Endpoint protection. Use the following procedure:

1. In the **Microsoft Endpoint Manager Admin Center**, click **Devices**, click **Windows**, and then click **Configuration profiles**.
2. Click **Create profile**.
3. On the **Create a profile** blade, in the **Platform** list, select **Windows 10 and later**, and then select the Profile type of **Templates**.
4. In the template list, click **Endpoint protection** and click **Create**.
5. On the **Basics** tab, enter a name and click **Next**.
6. On the **Configuration settings** tab, expand **Windows Encryption**.
7. In the **Windows Settings** section, select **Require** for the **Encrypt devices** value.

* You can go on to configure supplementary settings, such as requiring additional authentication at startup and supported encryption methods. However, you don’t have to.

1. Click **Next**, and then assign the profile to the appropriate user or device groups and complete the wizard.

The BitLocker recovery keys are automatically stored in Intune.

**Enabling BitLocker on removable storage**

It’s not difficult to lose an SD memory card or a USB memory stick. So, it makes sense to consider encrypting these removable storage devices. BitLocker makes this easy:

1. Open **File Explorer**and navigate to **This PC**.
2. Right-click the target storage device, and then select **Show more options**.
3. Click **Turn BitLocker** **on**. The BitLocker Drive Encryption wizard starts.
4. On the **Choose how you want to unlock this drive** page, select the **Use a password to unlock the drive**.

* You can’t use a TPM to unlock your removable storage device, so you can use either a smart card or a password to unlock it.

1. Enter the password you want to use, confirm the password, and then click **Next**.
2. On the **How do you want to back up your recovery key?** page, choose from:

* Save to your Microsoft account
* Save to a file
* Print the recovery key
* Your options might vary depending on the type of account you are signed in with.

1. Click **Next**, and BitLocker encryption starts.

**Recovering a BitLocker encrypted drive**

When enabling BitLocker, you’re usually prompted to store a recovery key. Depending on your device configuration, and the type of storage you’re encrypting, you’ll have several options for this. But how and when do you use the recovery key?

The recovery key is a 48-digit number divided into eight groups. During recovery, enter this key into the BitLocker Recovery Console.

When your computer starts, BitLocker checks the system integrity, as described earlier. If BitLocker detects a problem, it won’t unlock the Boot volume (the operating system drive C:), and it enters recovery mode. To enable the computer to start normally, you’ll need to enter the recovery key.

It would also be a pretty good idea to resolve the problem that caused BitLocker to enter recovery mode.

When you encrypt your Boot volume with BitLocker, you are prompted to store the recovery key. Depending on your computer’s configuration, you’ll be presented with several options including:

* Save to your Microsoft account
* Save to Active Directory Domain Services
* Save to a file
* Print the recovery key

**Situations where BitLocker might enter recovery mode**

There are several situations where BitLocker might enter recovery mode, including:

* Moving the BitLocker-encrypted drive to another computer, perhaps to recover its data.
* Powering off the computer off during the BitLocker encryption process.
* Updating your computer’s firmware.
* Changing the device boot order in the computer’s BIOS.
* You can inadvertently change the boot order by inserting removable storage devices, including smartphones.

In these situations, you’ll need the recovery key.

Lesson 4

**Implementing Windows 11 security features**

As security threats have evolved, so Windows has evolved. Windows 11 now includes a range of advanced security features that can help protect your computer from common security threats. These features include Microsoft Defender Credential Guard, and Microsoft Defender Exploit Guard.

Windows 11 also provides a unified interface for managing security settings. The Windows Security app provides access to all the most common security settings, including virus and threat protection, account protection, firewall settings, device security, and app and browser control.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe Microsoft Defender security features.
* Configure security settings using Windows Security.

**Overview of Windows 11 security features**

Windows 11 includes a wealth of security features to help protect your devices. We’ve already learned about Microsoft Defender Application Guard, which helps protect Microsoft Edge browsing sessions and Microsoft Office documents.

But Windows 11 includes many more security features, including:

* Microsoft Defender Credential Guard
* Microsoft Defender Exploit Guard
* Microsoft Defender for Endpoint
* Microsoft Defender Application Control
* Microsoft Defender Antivirus
* Windows Defender Firewall

The specific features you have depends on the Windows 11 edition you’re using. Windows 11 Enterprise supports all features.

**Microsoft Defender Credential Guard**

When you sign in to your Windows computer with a user name and password, the Local Security Authority (LSA) stores this information as hashes in memory while your entered credentials are verified by the appropriate authentication service.

The authentication service could be the local account database, Active Directory domain controller, or Azure Active Directory.

During the time that these hashes are in memory, there’s a small risk that any malicious code present in your computer might be able to exploit those hashes. To mitigate, you can enable Microsoft Defender Credential Guard.

Credential Guard, like Application Guard, is a virtualization-assisted security technology. In this instance, the virtualization is used to store the hashed credentials in an isolated, virtualized container. The host computer cannot access the contents of this container, thereby helping to protect these critical hashes.

Credential Guard requirements align with those for Application Guard, and your computer must have the following:

* Support for Virtualization-based security
* UEFI 2.3.1 or greater
* Secure Boot
* TPM 2.0, either discrete or firmware
* UEFI (firmware) lock
* Virtualization features, including SLAT, must be enabled

You can enable Credential Guard using Group Policy or by using an Intune Endpoint protection profile. To use Group Policy:

1. Open the appropriate GPO for editing, and navigate to **Computer Configuration / Policies / Administrative Templates / System / Device Guard**.
2. Double-click the **Turn On Virtualization Based Security** value.
3. In the **Turn On Virtualization Based Security** dialog box, select Enabled.
4. Under the **Credential Guard Configuration** heading, select **Enable with UEFI lock** and click **OK**.
5. Close the editor.

**Microsoft Defender Exploit Guard**

Exploit Guard helps reduce the attack surface of your computers. It provides four protections:

* **Exploit protection**. Leverages Microsoft Defender Antivirus to mitigate exploit techniques that might be used against your organization’s apps.
* **Attack surface reduction**. Helps protect against attack vectors that are delivered by scripts, email messages, and Office documents. Also based around Microsoft Defender Antivirus.
* **Network protection**. Uses Microsoft Defender SmartScreen technology in Microsoft Edge, and other apps, to limit and prohibit access to known unsafe web URLs and IP addresses. Also requires Microsoft Defender Antivirus and cloud-delivered protection must be enabled.
* **Controlled folder access**. Helps protect against malware and ransomware by preventing changes to specified folders. If Exploit Guard senses that apps are exhibiting malicious behavior, access is blocked. Also requires Microsoft Defender Antivirus.

For all but Exploit protection, your device must have Microsoft Defender for Endpoint always-on protection enabled.

You can configure Exploit Protection using the Windows Security app, Group Policy, or Microsoft Intune. You can configure Attack surface reduction, Network protection, and Controlled folder access using Configuration Manager or Intune.

**Using the Windows Security app**

In earlier versions of Windows, security-related settings were distributed through the operating system. These settings were accessible only by using a disparate collection of tools.

Windows 10 introduced the Windows Security app, a single point of contact for all security-related settings and tools. Windows Security provides consolidated access to the following:

* **Virus & threat protection**. Enables you to:
* Review current and past security threats
* Review allowed or quarantined threats
* Check protection history
* Configure virus and threat protection settings
* Perform an antivirus scan
* **Account protection**. Provides access to:
* Windows Hello settings
* Dynamic lock settings
* Sync settings for your account
* **Firewall & network protection**. Enables you to review current firewall status, and use links to:
* Allow an app through the firewall
* Run the Network and Internet troubleshooter
* Configure firewall notification settings
* Review and configure advanced settings (open Windows Firewall with Advanced Security)
* Restore settings to default values
* **App & browser control**. Provides access to:
* Reputation-based protection
* Isolated browsing (Application Guard)
* Exploit protection
* **Device security**. Enables you to review details about:
* Core isolation
* Security processor (TPM)
* Secure boot
* **Device performance and health**. Provides an at-a-glance health report on:
* Storage capacity
* Battery life
* Apps and software
* Windows Time service
* **Protection history**. Enables you to review the latest protection actions and recommendations generated by Windows Security.

Depending on the Windows 11 edition, you might also have a Family options tab.

Consider using Windows Security as your initial point of contact for security-related settings. You might then decide to switch to another, more specific management tool.

**Demonstration: Configuring Windows Security settings and features**

Lesson 5

**Securing against network threats**

You’ve already learned that your data is under threat at rest. But data is also under threat while in transit between devices, and between your device and on-premises or cloud-based services. By using Windows Defender Firewall, you can help to mitigate the network threats posed to your computer and its data.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe common network security threats.
* Configure Windows Defender Firewall.
* Configure Windows Defender Firewall with Advanced Security.

**What are the common network security threats?**

Your devices and services are at risk when connected to a network. The precise risks devices and services face depends on your infrastructure configuration, whether you’re connected to cloud services, and whether you allow guest connectivity to your network infrastructure.

It’s worth spending a moment to consider the types of threats that are posed by network connectivity. The following table outlines some of the more common threats.

|  |  |
| --- | --- |
| Threat | Explanation |
| Eavesdropping | Occurs when a malicious hacker captures network packets on your network. With WiFi connections, that’s easier than ever to achieve. Eavesdropping can enable access to sensitive data, such as user names and passwords, which in turn, can lead to other, more damaging attacks. |
| Denial of service (DoS) | Limits the function of a network app. Possibly makes an app or resource unavailable. Malicious hackers can use a variety of DoS attacks to target specific vulnerabilities in your apps and services. |
| Port scanning | Looks for TCP or UDP ports that are open on a specific device. Since many ports are well-known (for example, TCP port 443 is for secure web traffic), hackers can exploit the open port to enable more destructive attack techniques. |
| Man-in-the-middle | Enables a computer to impersonate another, legitimate computer on your network. Traffic can be directed to the impersonating device instead of the legitimate device. A malicious hacker might want to view the data in transit between the two hosts, or they might want to modify that data before onward forwarding. |

Being aware of common threats enables you to consider mitigations.

**Mitigations for network security threats**

You can use the following mitigations to help protect against these common threats:

* **Eavesdropping**. IP Security (IPsec), Virtual Private Networks (VPNs), and intruder detection.
* **DoS**. Firewalls, security zones, IPsec, and server hardening.
* **Port scanning**. Server hardening and firewalls.
* **Man-in-the-middle**. IPsec and DNSSEC.
* **Viruses or malicious code**. Antivirus and anti-malware software, and Windows updates.

The following table describes these mitigations in more detail.

|  |  |
| --- | --- |
| Mitigation | Explanation |
| IPsec | Provides for both authentication and optionally encryption for network traffic in transit between hosts, tunnel endpoints, and other scenarios. |
| Host firewalls | Enables you to allow or block network traffic based on that traffic’s characteristics, such as IP addresses, TCP or UDP ports, and so on. Host firewalls run as services on host computers. |
| Security zones | Provides a way to control the movement of traffic between designated areas. By using firewalls and other network devices, you can create zones such as internet, perimeter, and intranet. You can then define what type of traffic can flow in which direction between zones, and using which protocols and ports. |
| VPNs | Enables users to create a virtually secure connection across a public network. By using authentication, encryption, and encapsulation, users can seamlessly connect to their workplace network through devices placed in the perimeter zone. |
| Server hardening | Uses security baselines to determine which services are needed on your servers. Services that are not needed are not started. By initiating only the services you need, to reduce the attack surface of your servers. |
| Intrusion detection | Provides an ability to proactively look for intruders in your network instead of reacting only when something has happened. |
| DNSSEC | Domain Name System Security Extensions (DNSSEC) helps protect the DNS zones that are the foundation of name resolution in TCP-based networks. Helps client and server devices verify the authenticity of returned DNS records when performing name resolution. |

**Discussion: What security issues has your organization faced?**

**Configuring Windows Defender Firewall**

Windows Defender Firewall is a built-in host firewall solution in Windows client and Windows Server. Like all firewalls, the purpose of Windows Defender Firewall is to control the flow of network traffic in and out of the local host based on:

* Traffic details:
* Source address.
* Destination address.
* Source port.
* Destination port.
* Traffic protocol.
* Packet contents.

By default, Windows Defender Firewall is enabled by default, and configured with the most appropriate firewall rules for most situations. However, if you install additional apps or enable additional services, you’ll need to know how to configure the firewall.

**Network location profiles**

Windows Defender Firewall uses the network location profiles built-in to Windows 11. These profiles identify the type of network connection, and apply a generic collection of settings appropriate for that type of connection. The network location profiles are:

* **Public**. This is the default. When you first connect to a new network, the Public network location profile is assigned to it. You can change this to Private, or back to Public, by using the Settings app.
* **Private**. Choose this option if you’re connecting to a known network at your workplace or at home. Using this profile for connections to a public WiFi hotspot in a coffeeshop or airport is ill-advised.
* **Domain**. This is a variation of the Private network location profile. If you connect your domain-joined computer to your work network, the computer recognizes the network as being a domain network, and chooses that profile automatically.

Generally speaking, you’d enforce more strict firewall settings for the Public network location profile than for Private or Domain.

**Allowing an app through the firewall**

If you install an new app or enable a Windows feature, such as Remote Desktop, you might need to reconfigure your firewall settings. The easiest way to achieve this is to use Windows Security, and then use the following procedure:

1. Open **Windows Security** and then click **Firewall & network protection**.
2. Click the link for **Allow an app through the firewall**.
3. Switch to the **Allowed apps** dialog box.
4. Click the **Change** **settings** button, and if prompted by **User Account Control**, click **Yes**.

* Depending on your computer’s configuration, you’ll see 2 or 3 columns, one for each network location profile: Private, Public, and Domain. You can use the check boxes in each column for each app or feature to independently configure the firewall.

1. Scroll down the list of apps and features in the dialog box until you locate the appropriate one. Then select the **Private**, **Public**, and **Domain** check boxes as needed. Click **OK**.

If the app or feature you want isn’t listed:

1. Click **Allow another app**.
2. In the **Add an app** dialog box, browse to and select the executable name for the installed app.
3. In the **Add an app** dialog box, click **Add**.
4. In the **Allowed applications** dialog box, select the **Private**, **Public**, and **Domain** check boxes as needed. Click **OK**.

Generally, you should try to avoid manually configuring the firewall in these ways. It’s often the case that when you enable a Windows feature, the corresponding firewall exception is created automatically. For example, if you enable Remote Desktop in the Settings app, the corresponding firewall exception is enabled for you.

Likewise, if you enable Windows Remote Management (WinRM) by using the **WinRM QuickConfig** command at the Command Prompt, Windows Remote Management is enabled on the Private network location profile automatically. (This command also starts the WinRM listener service).

**Configuring Windows Defender Firewall with Advanced Security**

In some situations, you might want to manually configure your firewall by creating the necessary inbound and outbound rules. You might also want to implement IPsec to help protect against the network threats we discussed. In these circumstances, you’ll need to use Windows Defender Firewall with Advanced Security.

**Creating an inbound or outbound rule**

If you want to open a specific type of network traffic by direction and port rather than by selecting an app or feature, use the following procedure:

1. Open **Windows Security** and then click **Firewall & network protection**.
2. Click the link for **Advanced settings**.
3. If prompted by **User Account Control**, click **Yes**.

To create an inbound rule, perform the following steps:

1. In **Windows Defender Firewall with Advanced Security**, click and then right-click the **Inbound Rules** node and choose **New Rule**.
2. In the **New Inbound Rule Wizard**, on the **Rule Type** page, choose **Custom** and click **Next**.

* You can also choose Program, Port, or Predefined. Program and Predefined are easier to configure using the Allow app or feature method.

1. On the **Program** page, click **Next**.
2. On the **Protocols and Ports** page, select the appropriate **Protocol type**, and if needed, **Local port** and **Remote port**. Click **Next**.
3. If you want to scope to the rule to specified IP addresses or ranges, on the **Scope** page, configure the required values. In most situations when configuring an individual computer, that’s not usually necessary. Click **Next**.
4. On the **Action** page, select one of the following actions, and then click **Next**:

* Allow the connection
* Allow the connection if it is secure
* Block the connection

1. On the **Profile** page, choose the network location profiles to which this rule applies and click **Next**.
2. Finally, on the **Name** page, enter a name and description and then click **Finish**.

Your rule displays in the console.

Allowed rules display a green circle with a white check mark. Blocked rules show a no entry sign. IPsec secured rules display a padlock.

Outbound rules follow a very similar procedure, but you’re controlling the outbound flow of the designated traffic.

**Creating a connection security rule**

It’s typical to use firewall rules and connection security rules together. For example, you might create a firewall rule that only allows traffic if it’s secured. You’ll then create a connection security rule that applies the required security.

Connection security rules secure traffic as it crosses a network by using IPsec. When you create a connection security rule, you define the type of connection, and then stipulate the method of authentication required.

Windows Defender Firewall supports a number of different scenarios for connection security rules:

* **Isolation**. Restrict connections based on authentication criteria, such as domain membership or health status.
* **Authentication exemption**. Define connections that don’t require authentication. This might be useful for infrastructure services, such as DHCP servers, domain controllers, or certification authorities.
* **Server-to-server**. Provide authenticated connections between designated computers.
* **Tunnel**. Provide secure communications between server two endpoints, typically at each end of a secure tunnel connection.
* **Custom**. Enable you to define the specific characteristics that you need for your rule.

To create a typical connection security rule, use the following procedure:

1. In **Windows Defender Firewall with Advanced Security**, click and then right-click the **Connection Security Rules** node and choose **New Rule**.
2. In the **New Connection Security Rule Wizard**, on the **Rule Type** page, choose **Server-to-server** and click **Next**.
3. On the **Endpoints** page, if necessary, enter the IP addresses or range of IP addresses for hosts that are targeted by this rule and click **Next**.

* This is not always needed as you can target the rule by using Group Policy settings.

1. On the **Requirements** page, choose the authentication requirements and then click **Next**:

* Request authentication for inbound and outbound connections
* Require authentication for inbound connections and request authentication for outbound connections
* Require authentication for inbound and outbound connections

1. On the **Authentication Method** page, choose one (or more) authentication methods and click **Next**. If you choose a Computer certificate, which is common, you must choose the appropriate CA name.
2. On the **Profile** page, choose the network location profiles to which this rule applies and click **Next**.
3. Finally, on the **Name** page, enter a name and description and then click **Finish**.

You can monitor the rule’s behavior using the Monitoring node.

It’s worth remembering that you can use Group Policy to configure inbound, outbound, and connection security rules. This enables you to configure multiple computers in a single step.

**Managing Windows Defender Firewall with Windows PowerShell**

The Windows PowerShell cmdlets described in the following table enable you to manage Windows Defender Firewall inbound and outbound rules.

|  |  |
| --- | --- |
| Windows PowerShell cmdlet | Description |
| Get-NetFirewallRule | Displays the available firewall rules |
| Copy-NetFirewallRule | Copies a firewall rule |
| Enable-NetFirewallRule | Enables a firewall rule |
| Disable-NetFirewallRule | Disables a firewall rule |
| New-NetFirewallRule | Creates a new firewall rule |
| Remove-NetFirewallRule | Deletes a firewall rule |
| Rename-NetFirewallRule | Renames a firewall rule |
| Set-NetFirewallRule | Configures the properties of a firewall rule |
| Show-NetFirewallRule | Lists all firewall rules |

The Windows PowerShell cmdlets described in the following table enable you to manage Windows Defender Firewall connection security rules.

|  |  |
| --- | --- |
| Windows PowerShell cmdlet | Description |
| Get-NetIPSecRule | Displays a list of connection security rules |
| Copy-NetIPSecRule | Copies a connection security rule |
| Enable-NetIPSecRule | Enables a connection security |
| Disable-NetIPSecRule | Disables a connection security rule |
| New-NetIPSecRule | Creates a connection security rule |
| Remove-NetIPSecRule | Deletes a connection security rule |
| Rename-NetIPSecRule | Renames a connection security rule |
| Set-NetIPSecRule | Configures the properties of a connection security rule |
| Show-NetIPSecRule | List all connection security rules |

**Demonstration: Configuring Windows Defender Firewall**

**Lab: Implementing and managing security**

**Question:**In the lab, you configured BitLocker. What’s the primary purpose of BitLocker?

**Module Review and Takeaways**

Review Questions

**Question:**There are two types of Microsoft account that you can add to a Windows 11 computer. What are they are how are they used?

**Question:**What kind of group is Authenticated Users?

**Question:**You want to protect your users’ browser sessions. Which Microsoft Defender feature could you implement in Windows 11?