Protect against security threats on Azure

Learn how Azure can help you protect the workloads that you run both in the cloud and in your on-premises datacenter.

Learning objectives

After completing this module, you'll be able to:

- Strengthen your security posture and protect against threats by using Azure Security Center.
- Collect and act on security data from many different sources by using Azure Sentinel.
- Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.

Introduction

In this module, you'll learn about some of the security tools that can help keep your infrastructure and data safe when you work in the cloud.

Security is a small word for a significant concept. There are so many factors to consider in order to protect your applications and your data. How does Azure help you protect workloads that you run in the cloud and in your on-premises datacenter?

Meet Tailwind Traders

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders run securely in the cloud and in the datacenter?

Tailwind Traders runs a mix of workloads on Azure and in its datacenter.

The company needs to ensure that all of its systems meet a minimum level of security, and that its information is protected from attacks. The company also needs a way to collect and act on security events from across its digital estate.

Let's explore how Tailwind Traders can use some of the tools and features in Azure as part of its overall security strategy.

Learning objectives

After completing this module, you'll be able to:

- Strengthen your security posture and protect against threats by using Azure Security Center.
- Collect and act on security data from many different sources by using Azure Sentinel.
- Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

A1: Protect against security threats by using Azure Security Center

Tailwind Traders is broadening its use of Azure services. It still has on-premises workloads with current security-related configuration best practices and business procedures. How does the company ensure that all of its systems meet a minimum level of security and that its information is protected from attacks?

Many Azure services include built-in security features. Tools on Azure can also help Tailwind Traders with this requirement. Let's start by looking at Azure Security Center.

What's Azure Security Center?

Azure Security Center is a monitoring service that provides visibility of your security posture across all of your services, both on Azure and on-premises. The term *security posture* refers to cybersecurity policies and controls, as well as how well you can predict, prevent, and respond to security threats.

Security Center can:

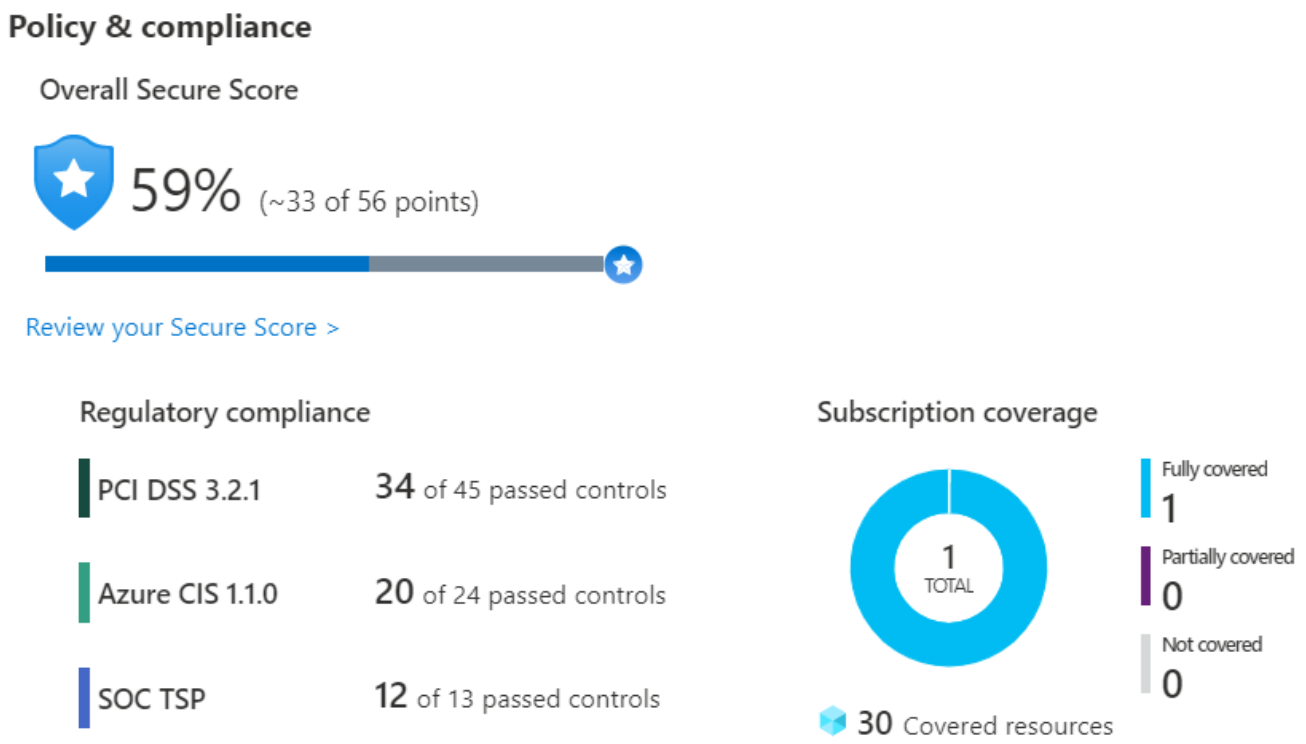
- Monitor security settings across on-premises and cloud workloads.
- Automatically apply required security settings to new resources as they come online.
- Provide security recommendations that are based on your current configurations, resources, and networks.
- Continuously monitor your resources and perform automatic security assessments to identify potential vulnerabilities before those vulnerabilities can be exploited.
- Use machine learning to detect and block malware from being installed on your virtual machines (VMs) and other resources. You can also use *adaptive application controls* to define rules that list allowed applications to ensure that only applications you allow can run.
- Detect and analyze potential inbound attacks and investigate threats and any post-breach activity that might have occurred.
- Provide just-in-time access control for network ports. Doing so reduces your attack surface by ensuring that the network only allows traffic that you require at the time that you need it to.

This short video explains how Security Center can help harden your networks, secure and monitor your cloud resources, and improve your overall security posture.

Understand your security posture

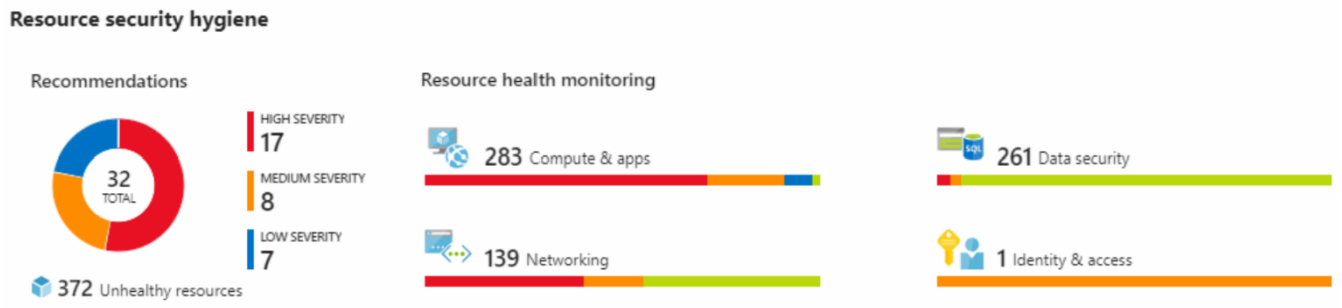
Tailwind Traders can use Security Center to get a detailed analysis of different components in its environment. Because the company's resources are analyzed against the security controls of any governance policies it has assigned, it can view its overall regulatory compliance from a security perspective all from one place.

See the following example of what you might see in Azure Security Center.



Let's say that Tailwind Traders must comply with the Payment Card Industry's Data Security Standard (PCI DSS). This report shows that the company has resources that it needs to remediate.

In the **Resource security hygiene** section, Tailwind Traders can see the health of its resources from a security perspective. To help prioritize remediation actions, recommendations are categorized as low, medium, and high. Here's an example.

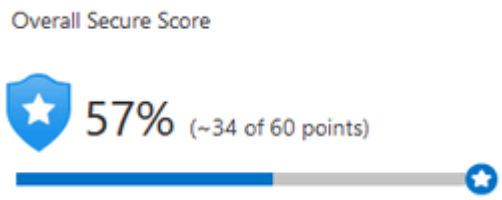


What's secure score?

Secure score is a measurement of an organization's security posture.

Secure score is based on *security controls*, or groups of related security recommendations. Your score is based on the percentage of security controls that you satisfy. The more security controls you satisfy, the higher the score you receive. Your score improves when you remediate all of the recommendations for a single resource within a control.

Here's an example from the Azure portal showing a score of 57 percent, or 34 out of 60 points.



Following the secure score recommendations can help protect your organization from threats. From a centralized dashboard in Azure Security Center, organizations can monitor and work on the security of their Azure resources like identities, data, apps, devices, and infrastructure.

Secure score helps you:

- Report on the current state of your organization's security posture.
- Improve your security posture by providing discoverability, visibility, guidance, and control.
- Compare with benchmarks and establish key performance indicators (KPIs).

Protect against threats

Security Center includes advanced cloud defense capabilities for VMs, network security, and file integrity. Let's look at how some of these capabilities apply to Tailwind Traders.

- **Just-in-time VM access** Tailwind Traders will configure just-in-time access to VMs. This access blocks traffic by default to specific network ports of VMs, but allows traffic for a specified time when an admin requests and approves it.
- **Adaptive application controls** Tailwind Traders can control which applications are allowed to run on its VMs. In the background, Security Center uses machine learning to look at the processes running on a VM. It creates exception rules for each resource group that holds the VMs and provides recommendations. This process provides alerts that inform the company about unauthorized applications that are running on its VMs.
- **Adaptive network hardening** Security Center can monitor the internet traffic patterns of the VMs, and compare those patterns with the company's current network security group (NSG) settings. From there, Security Center can make recommendations about whether the NSGs should be locked down further and provide remediation steps.
- **File integrity monitoring** Tailwind Traders can also configure the monitoring of changes to important files on both Windows and Linux, registry settings, applications, and other aspects that might indicate a security attack.

Respond to security alerts

Tailwind Traders can use Security Center to get a centralized view of all of its security alerts. From there, the company can dismiss false alerts, investigate them further, remediate alerts manually, or use an automated response with a *workflow automation*.

Workflow automation uses Azure Logic Apps and Security Center connectors. The logic app can be triggered by a threat detection alert or by a Security Center recommendation, filtered by name or by severity. You can then configure the logic app to run an action, such as sending an email, or posting a message to a Microsoft Teams channel.

A2: Detect and respond to security threats by using Azure Sentinel

Security management on a large scale can benefit from a dedicated security information and event management (SIEM) system. A SIEM system aggregates security data from many different sources (as long as those sources support an open-standard logging format). It also provides capabilities for threat detection and response.

Azure Sentinel is Microsoft's cloud-based SIEM system. It uses intelligent security analytics and threat analysis.

Azure Sentinel capabilities

Azure Sentinel enables you to:

- **Collect cloud data at scale** Collect data across all users, devices, applications, and infrastructure, both on-premises and from multiple clouds.
- **Detect previously undetected threats** Minimize false positives by using Microsoft's comprehensive analytics and threat intelligence.
- **Investigate threats with artificial intelligence** Examine suspicious activities at scale, tapping into years of cybersecurity experience from Microsoft.
- **Respond to incidents rapidly** Use built-in orchestration and automation of common tasks.

Connect your data sources

Tailwind Traders decides to explore the capabilities of Azure Sentinel. First, the company identifies and connects its data sources.

Azure Sentinel supports a number of data sources, which it can analyze for security events. These connections are handled by built-in connectors or industry-standard log formats and APIs.

- **Connect Microsoft solutions** Connectors provide real-time integration for services like Microsoft Threat Protection solutions, Microsoft 365 sources (including Office 365), Azure Active Directory, and Windows Defender Firewall.
- **Connect other services and solutions** Connectors are available for common non-Microsoft services and solutions, including AWS CloudTrail, Citrix Analytics (Security), Sophos XG Firewall, VMware Carbon Black Cloud, and Okta SSO.

- **Connect industry-standard data sources** Azure Sentinel supports data from other sources that use the Common Event Format (CEF) messaging standard, Syslog, or REST API.

Detect threats

Tailwind Traders needs to be notified when something suspicious occurs. It decides to use both built-in analytics and custom rules to detect threats.

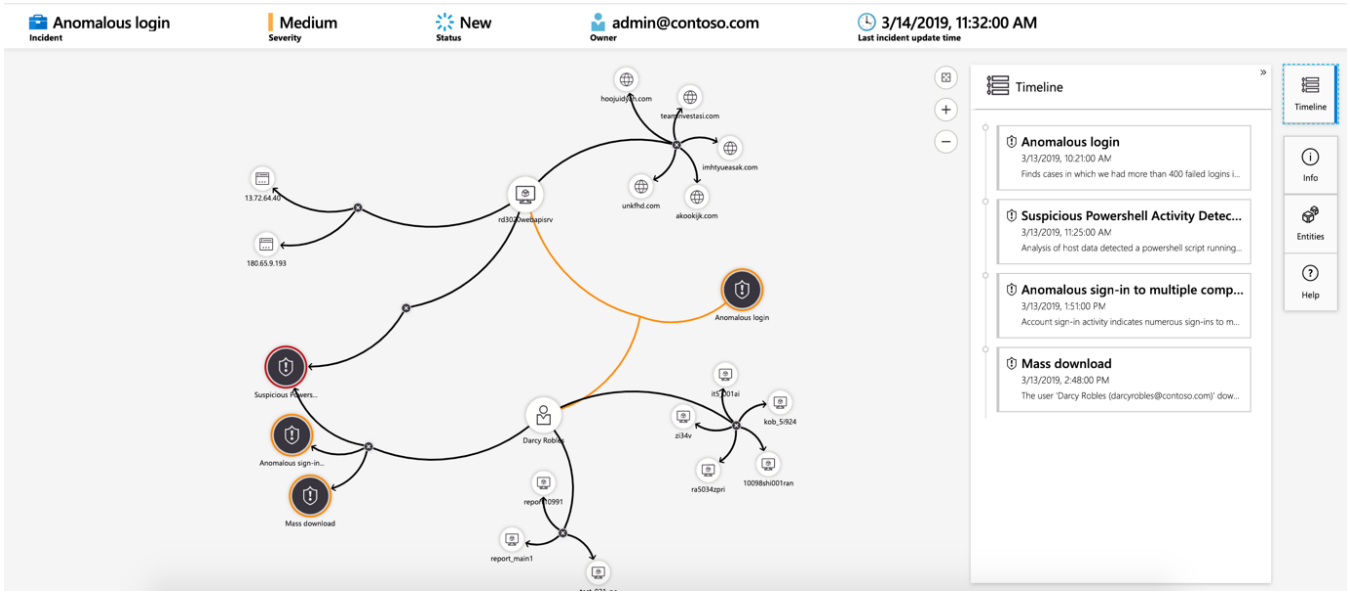
Built in analytics use templates designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and escalation chains for suspicious activity. These templates can be customized and search across the environment for any activity that looks suspicious. Some templates use machine learning behavioral analytics that are based on Microsoft proprietary algorithms.

Custom analytics are rules that you create to search for specific criteria within your environment. You can preview the number of results that the query would generate (based on past log events) and set a schedule for the query to run. You can also set an alert threshold.

Investigate and respond

When Azure Sentinel detects suspicious events, Tailwind Traders can investigate specific alerts or *incidents* (a group of related alerts). With the investigation graph, the company can review information from entities directly connected to the alert, and see common exploration queries to help guide the investigation.

Here's an example that shows what an investigation graph looks like in Azure Sentinel.



The company will also use Azure Monitor Workbooks to automate responses to threats. For example, it can set an alert that looks for malicious IP addresses that access the network and create a workbook that does the following steps:

1. When the alert is triggered, open a ticket in the IT ticketing system.

2. Send a message to the security operations channel in Microsoft Teams or Slack to make sure the security analysts are aware of the incident.
3. Send all of the information in the alert to the senior network admin and to the security admin. The email message includes two user option buttons: **Block** or **Ignore**.

When an admin chooses **Block**, the IP address is blocked in the firewall, and the user is disabled in Azure Active Directory. When an admin chooses **Ignore**, the alert is closed in Azure Sentinel, and the incident is closed in the IT ticketing system.
The workbook continues to run after it receives a response from the admins.
Workbooks can be run manually or automatically when a rule triggers an alert.

A3: Store and manage secrets by using Azure Key Vault

As Tailwind Traders builds its workloads in the cloud, it needs to carefully handle sensitive information such as passwords, encryption keys, and certificates. This information needs to be available for an application to function, but it might allow an unauthorized person access to application data.

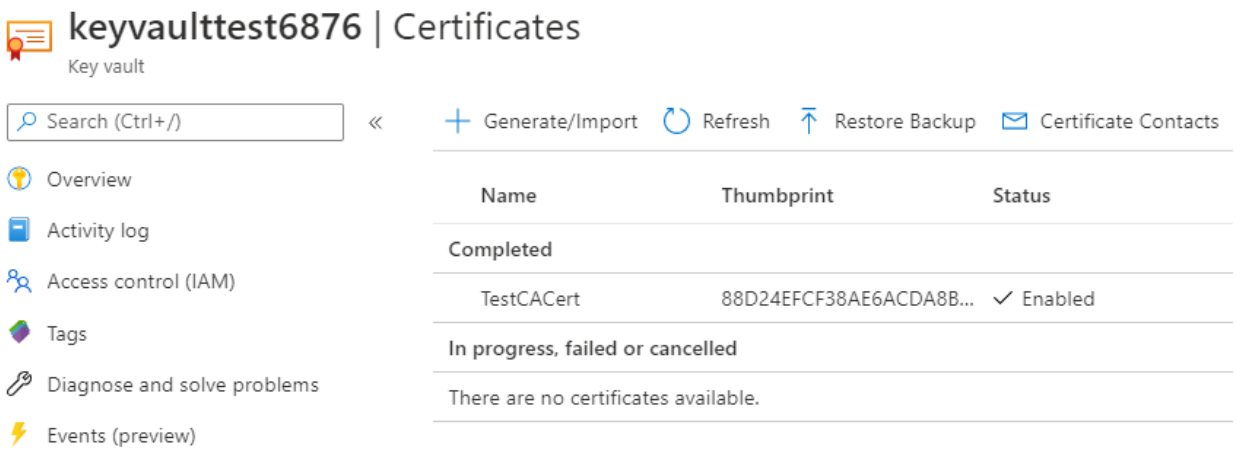
Azure Key Vault is a centralized cloud service for storing an application's secrets in a single, central location. It provides secure access to sensitive information by providing access control and logging capabilities.

What can Azure Key Vault do?

Azure Key Vault can help you:

- **Manage secrets** You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.
- **Manage encryption keys** You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys that are used to encrypt your data.
- **Manage SSL/TLS certificates** Key Vault enables you to provision, manage, and deploy your public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for both your Azure resources and your internal resources.
- **Store secrets backed by hardware security modules (HSMs)** These secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

Here's an example that shows a certificate used for testing in Key Vault.



You'll add a secret to Key Vault later in this module.

What are the benefits of Azure Key Vault?

The benefits of using Key Vault include:

- **Centralized application secrets** Centralizing the storage for your application secrets enables you to control their distribution, and reduces the chances that secrets are accidentally leaked.
- **Securely stored secrets and keys** Azure uses industry-standard algorithms, key lengths, and HSMs. Access to Key Vault requires proper authentication and authorization.
- **Access monitoring and access control** By using Key Vault, you can monitor and control access to your application secrets.
- **Simplified administration of application secrets** Key Vault makes it easier to enroll and renew certificates from public certificate authorities (CAs). You can also scale up and replicate content within regions and use standard certificate management tools.
- **Integration with other Azure services** You can integrate Key Vault with storage accounts, container registries, event hubs, and many more Azure services. These services can then securely reference the secrets stored in Key Vault.

Exercise - Manage a password in Azure Key Vault

In this exercise, you add a password to Azure Key Vault. A password is an example of sensitive information that you need to protect. You then read the password from Azure Key Vault to verify that the password is accessible.

In practice, there are several ways to add secrets to and read secrets from Key Vault. You can use the Azure portal, the Azure CLI, or Azure PowerShell. By using your favorite programming language, your applications can also securely access the secrets that they need.

Here, you create a secret in Key Vault by using the Azure portal. You then access the secret from the portal and from the Azure CLI in Azure Cloud Shell.

The Azure CLI is a way to work with Azure resources from the command line or from scripts. Cloud Shell is a browser-based shell experience to manage and develop Azure resources. Think of Cloud Shell as an interactive console that runs in the cloud.

Create a key vault

1. Go to the Azure portal.
2. On the Azure portal menu, or from the **Home** page, under **Azure services**, select **Create a resource**. The **Create a resource** pane appears.
3. In the search bar, enter *Key Vault*, and then select **Key Vault** from the results. **The Key Vault** pane appears.
4. Select **Create**. The **Create a key vault** pane appears.
5. On the **Basics** tab, enter the following values for each setting.

   Note

Replace *NNN* with a series of numbers. This helps ensure that the name of your key vault is unique.

Setting	Value
Project details	
Subscription	Concierge Subscription
Resource group	[sandbox resource group name]
Instance details	
Key vault name	my-keyvault-NNN where NNN is a unique identifier

Accept the remaining settings at their default values.

6. Select **Review + create**, and after passing validation, select **Create**.

   Wait for deployment to successfully complete.
7. Select **Go to resource**.
8. Take note of some of the details about your key vault.

   For example, the **Vault URI** field shows the URI that your application can use to access your vault from the REST API.

   Here's an example for a key vault that's named **my-keyvault-321**:

9. As an optional step, on the left menu pane, under **Settings**, examine some of the other features.

   Although they're initially empty, here you'll find places where you can store keys, secrets, and certificates.

   Note

   Your Azure subscription is the only one that's authorized to access this vault. Under **Settings**, the **Access policies** feature enables you to configure access to the vault.

Add a password to the key vault

1. On the left menu pane, under **Settings**, select **Secrets**. Your key vault pane appears.
2. From the top menu bar, select **Generate/Import**. The **Create a secret** pane appears.

3. Fill in the following values for each setting.

Setting	Value
Upload options	Manual
Name	MyPassword
Value	hVFkk96

4. Accept the remaining settings at their default values. Notice that you can specify properties such as the activation date and the expiration date. You can also disable access to the secret.

5. Select **Create**.

Show the password

Here, you access the password from Key Vault two times. First, you access it from the Azure portal. Next, you access it from the Azure CLI.

1. From your **Key Vault/Secrets** pane, select **MyPassword**. The **MyPassword/Versions** pane appears. You see that the current version is enabled.

2. Select the current version. The **Secret Version** pane appears.

   Under **Secret Identifier**, you see a URI that you can now use with applications to access the secret. Remember, only authorized applications can access this secret.

3. Select **Show Secret Value**. The unique value for this version of the password appears.

4. From Cloud Shell, run this command.

   Note

   Replace **my-keyvault-NNN** with the name you used earlier.

   Azure CLICopy

```
az keyvault secret show \
    --name MyPassword \
    --vault-name my-keyvault-NNN \
    --query value \
    --output tsv
```

   You see the password in the output.

   OutputCopy

```
hVFkk96
```

Good work! At this point, you have a key vault that contains a password secret that's securely stored for use with your applications.

Clean up

The sandbox automatically cleans up your resources when you're finished with this module.

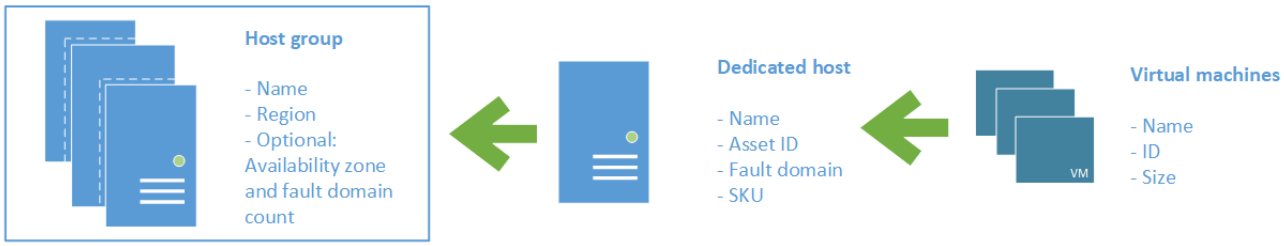
When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

Host your Azure virtual machines on dedicated physical servers by using Azure Dedicated Host

On Azure, virtual machines (VMs) run on shared hardware that Microsoft manages. Although the underlying hardware is shared, your VM workloads are isolated from workloads that other Azure customers run.

Some organizations must follow regulatory compliance that requires them to be the only customer using the physical machine that hosts their virtual machines. Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

Here's a diagram that shows how VMs relate to dedicated hosts and host groups. A *dedicated host* is mapped to a physical server in an Azure datacenter. A *host group* is a collection of dedicated hosts.



What are the benefits of Azure Dedicated Host?

Azure Dedicated Host:

- Gives you visibility into, and control over, the server infrastructure that's running your Azure VMs.
- Helps address compliance requirements by deploying your workloads on an isolated server.
- Lets you choose the number of processors, server capabilities, VM series, and VM sizes within the same host.

Availability considerations for Dedicated Host

After a dedicated host is provisioned, Azure assigns it to the physical server in Microsoft's cloud datacenter.

For high availability, you can provision multiple hosts in a *host group*, and deploy your VMs across this group. VMs on dedicated hosts can also take advantage of *maintenance control*. This feature enables you to control when regular maintenance updates occur, within a 35-day rolling window.

Pricing considerations

You're charged per dedicated host, independent of how many VMs you deploy to it. The host price is based on the VM family, type (hardware size), and region.

Software licensing, storage, and network usage are billed separately from the host and VMs. For more information. see Azure Dedicated Host pricing.

Knowledge check

Consider the following scenario.

Tailwind Traders is moving its online payment system from its datacenter to the cloud. The payment system consists of virtual machines (VMs) and SQL Server databases.

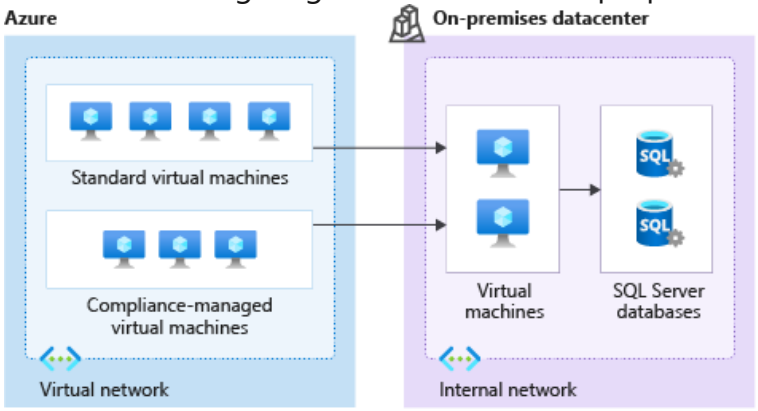
Here are a few security requirements that the company identifies as it plans the migration:

- It wants to ensure a good security posture across all of its systems, both on Azure and on-premises.
- In the datacenter, access to VMs requires a TLS certificate. The company needs a place to safely store and manage its certificates.

Here are some additional requirements that relate to regulatory compliance:

- Tailwind Traders must store certain customer data on-premises, in its datacenter.
- For certain workloads, the company must be the only customer running VMs on the physical hardware.
- The company must only run approved business applications on each VM.

See the following diagram that shows the proposed architecture.



On Azure, Tailwind Traders will use both standard VMs and VMs that run on dedicated physical hardware. In the datacenter, the company will run VMs that can connect to databases within its internal network.

Choose the best response for each question. Then select **Check your answers**.

Check your knowledge

1. How can Tailwind Traders enforce having only certain applications run on its VMs?

- Connect your VMs to Azure Sentinel.
- Create an application control rule in Azure Security Center.
- Periodically run a script that lists the running processes on each VM. The IT manager can then shut down any applications that shouldn't be running.

2. What's the easiest way for Tailwind Traders to combine security data from all of its monitoring tools into a single report that it can take action on?

- Collect security data in Azure Sentinel.
- Build a custom tool that collects security data, and displays a report through a web application.
- Look through each security log daily and email a summary to your team.

3. Which is the best way for Tailwind Traders to safely store its certificates so that they're accessible to cloud VMs?

- Place the certificates on a network share.
- Store them on a VM that's protected by a password.
- Store the certificates in Azure Key Vault.

4. How can Tailwind Traders ensure that certain VM workloads are physically isolated from workloads being run by other Azure customers?

- Configure the network to ensure that VMs on the same physical host are isolated.
- This is not possible. These workloads need to be run on-premises.
- Run the VMs on Azure Dedicated Host.

Summary

Tailwind Traders faces a number of security challenges. In today's digital world, its needs aren't unique.

Azure provides tools and services that can help you detect and act on important security events. It also provides ways to help keep your data safe, which can prevent security incidents from happening to begin with.

In this module, you learned about Azure services that relate to security. Here's a brief summary:

- Azure Security Center provides visibility of your security posture across all of your services, both on Azure and on-premises.
- Azure Sentinel aggregates security data from many different sources, and provides additional capabilities for threat detection and response.
- Azure Key Vault stores your applications' secrets, such as passwords, encryption keys, and certificates, in a single, central location.
- Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

Learn more

Here are more resources to help you go further.

Azure Security Center

Take the Resolve security threats with Azure Security Center module to use the alert capabilities of Azure Security Center to watch for and respond to threats.
Then review the planning and operations guide to optimize your use of Security Center based on your organization's security requirements and cloud management model.

Azure Sentinel

Design a holistic monitoring strategy on Azure goes into greater depth on how Azure Sentinel can help monitor and respond to security threats across your organization.
Also learn how to connect data sources to Azure Sentinel.

Azure Key Vault

Gain additional hands-on experience with Azure Key Vault in Manage secrets in your server apps with Azure Key Vault and Configure and manage secrets in Azure Key Vault.

Secure network connectivity on Azure

Learn about the Azure services you can use to help ensure that your network is safe, secure, and trusted.

Learning objectives

After completing this module, you'll be able to:

- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources within a Microsoft Azure virtual network.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.

Introduction

Every application and service, whether on-premises or in the cloud, needs to be designed with security in mind. There's too much at risk. For example, a denial-of-service attack might prevent customers from reaching your website or services and block you from doing business. Or, your website might be defaced, causing damage to your reputation. A data breach would be even worse, because it can ruin hard-earned trust while causing significant personal and financial harm.

Meet Tailwind Traders

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders secure its networks?

As Tailwind Traders moves to the cloud, it needs to evaluate its security needs before it can deploy a single line of code to production.

Although security must be considered at every layer in the company's applications (all the way from the physical servers to the application data), some factors relate specifically to the network configuration and network traffic of cloud-based workloads.

In this module, you'll focus on the network security capabilities in Azure and review how they help you secure your solutions in the cloud, based on your business needs.

Learning objectives

After completing this module, you'll be able to:

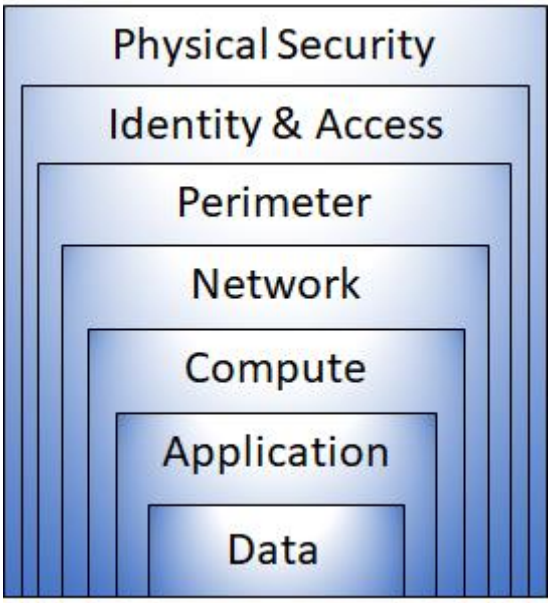
- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources within a Microsoft Azure virtual network.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

What is defense in depth?

Tailwind Traders currently runs its workloads on-premises, in its datacenter. Running on-premises means that the company is responsible for all aspects of security, from physical access to buildings all the way down to how data travels in and out of the network. The company wants to know how its current defense-in-depth strategy compares to running in the cloud.



The objective of *defense in depth* is to protect information and prevent it from being stolen by those who aren't authorized to access it.

A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data.

Layers of defense in depth

You can visualize defense in depth as a set of layers, with the data to be secured at the center.

Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert telemetry that security teams can act upon, either automatically or manually.

Here's a brief overview of the role of each layer:

- The *physical security* layer is the first line of defense to protect computing hardware in the datacenter.

- The *identity and access* layer controls access to infrastructure and change control.
- The *perimeter* layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- The *network* layer limits communication between resources through segmentation and access controls.
- The *compute* layer secures access to virtual machines.
- The *application* layer helps ensure that applications are secure and free of security vulnerabilities.
- The *data* layer controls access to business and customer data that you need to protect.

These layers provide a guideline for you to help make security configuration decisions in all of the layers of your applications.

Azure provides security tools and features at every level of the defense-in-depth concept. Let's take a closer look at each layer:

Physical security

Physically securing access to buildings and controlling access to computing hardware within the datacenter are the first line of defense.

With physical security, the intent is to provide physical safeguards against access to assets. These safeguards ensure that other layers can't be bypassed, and loss or theft is handled appropriately. Microsoft uses various physical security mechanisms in its cloud datacenters.

Identity and access

At this layer, it's important to:

- Control access to infrastructure and change control.
- Use single sign-on (SSO) and multifactor authentication.
- Audit events and changes.

The identity and access layer is all about ensuring that identities are secure, access is granted only to what's needed, and sign-in events and changes are logged.

Perimeter

At this layer, it's important to:

- Use DDoS protection to filter large-scale attacks before they can affect the availability of a system for users.
- Use perimeter firewalls to identify and alert on malicious attacks against your network.

At the network perimeter, it's about protecting from network-based attacks against your resources. Identifying these attacks, eliminating their impact, and alerting you when they happen are important ways to keep your network secure.

Network

At this layer, it's important to:

- Limit communication between resources.
- Deny by default.
- Restrict inbound internet access and limit outbound access where appropriate.
- Implement secure connectivity to on-premises networks.

At this layer, the focus is on limiting the network connectivity across all your resources to allow only what's required. By limiting this communication, you reduce the risk of an attack spreading to other systems in your network.

Compute

At this layer, it's important to:

- Secure access to virtual machines.
- Implement endpoint protection on devices and keep systems patched and current.

Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure that your compute resources are secure and that you have the proper controls in place to minimize security issues.

Application

At this layer, it's important to:

- Ensure that applications are secure and free of vulnerabilities.
- Store sensitive application secrets in a secure storage medium.
- Make security a design requirement for all application development.

Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in code. Every development team should ensure that its applications are secure by default.

Data

In almost all cases, attackers are after data:

- Stored in a database.
- Stored on disk inside virtual machines.
- Stored in software as a service (SaaS) applications, such as Office 365.
- Managed through cloud storage.

Those who store and control access to data are responsible for ensuring that it's properly secured. Often, regulatory requirements dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.

Security posture

Your *security posture* is your organization's ability to protect from and respond to security threats. The common principles used to define a security posture are *confidentiality*, *integrity*, and *availability*, known collectively as CIA.

- **Confidentiality**

  The *principle of least privilege* means restricting access to information only to individuals explicitly granted access, at only the level that they need to perform their work. This information includes protection of user passwords, email content, and access levels to applications and underlying infrastructure.

- **Integrity**

  Prevent unauthorized changes to information:

  - At rest: when it's stored.
  - In transit: when it's being transferred from one place to another, including from a local computer to the cloud.

  A common approach used in data transmission is for the sender to create a unique fingerprint of the data by using a one-way hashing algorithm. The hash is sent to the receiver along with the data. The receiver recalculates the data's hash and compares it to the original to ensure that the data wasn't lost or modified in transit.

- **Availability**

  Ensure that services are functioning and can be accessed only by authorized users. *Denial-of-service attacks* are designed to degrade the availability of a system, affecting its users.

Protect virtual networks by using Azure Firewall

A *firewall* is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. You can create firewall rules that specify ranges of IP addresses. Only clients granted IP addresses from within those ranges are allowed to access the destination server. Firewall rules can also include specific network protocol and port information.

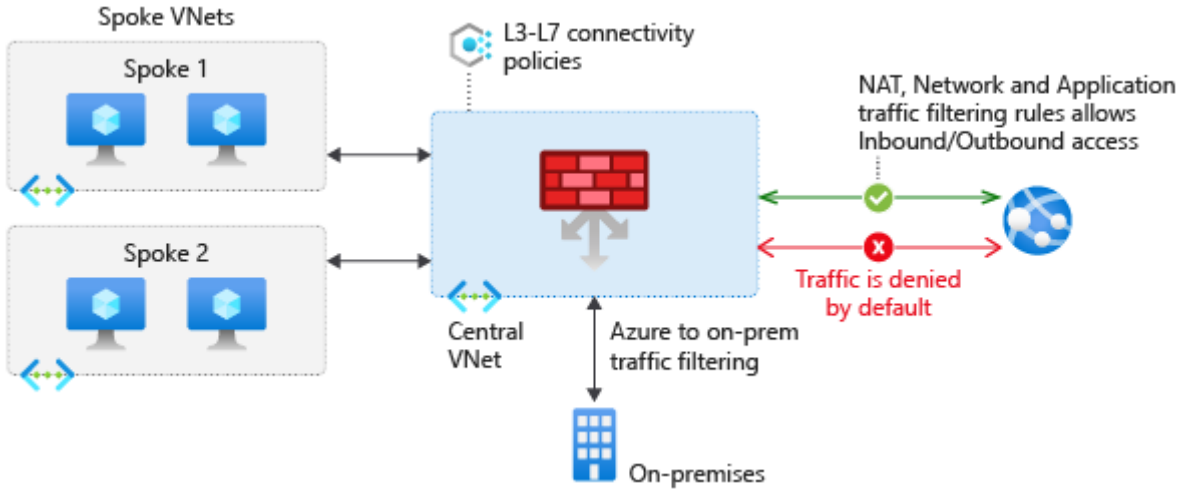
Tailwind Traders currently runs firewall appliances, which combine hardware and software, to protect its on-premises network. These firewall appliances require a monthly licensing fee to operate, and they require IT staff to perform routine maintenance. As Tailwind Traders moves to the cloud, the IT manager wants to know what Azure services can protect both the company's cloud networks and its on-premises networks.

In this part, you explore Azure Firewall.

What's Azure Firewall?

Azure Firewall is a managed, cloud-based network security service that helps protect resources in your Azure virtual networks. A virtual network is similar to a traditional network that you'd operate in your own datacenter. It's a fundamental building block for your private network that enables virtual machines and other compute resources to securely communicate with each other, the internet, and on-premises networks.

Here's a diagram that shows a basic Azure Firewall implementation:



Azure Firewall is a *stateful* firewall. A stateful firewall analyzes the complete context of a network connection, not just an individual packet of network traffic. Azure Firewall features high availability and unrestricted cloud scalability.

Azure Firewall provides a central location to create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static (unchanging) public IP address for your virtual network resources, which enables outside firewalls to identify traffic coming from your virtual network. The service is integrated with Azure Monitor to enable logging and analytics.

Azure Firewall provides many features, including:

- Built-in high availability.
- Unrestricted cloud scalability.
- Inbound and outbound filtering rules.
- Inbound Destination Network Address Translation (DNAT) support.
- Azure Monitor logging.

You typically deploy Azure Firewall on a central virtual network to control general network access.

This short video explains how Azure Firewall monitors incoming and outgoing network traffic based a defined set of security rules. The video also explains how Azure Firewall compares to traditional firewall appliances.

What can I configure with Azure Firewall?

With Azure Firewall, you can configure:

- Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
- Network rules that define source address, protocol, destination port, and destination address.
- Network Address Translation (NAT) rules that define destination IP addresses and ports to translate inbound requests.

Azure Application Gateway also provides a firewall that's called the *web application firewall* (WAF). WAF provides centralized, inbound protection for your web applications against common exploits and vulnerabilities. Azure Front Door and Azure Content Delivery Network also provide WAF services.

Protect from DDoS attacks by using Azure DDoS Protection

Any large company can be the target of a large-scale network attack. Tailwind Traders is no exception. Attackers might flood your network to make a statement or simply for the challenge. As Tailwind Traders moves to the cloud, it wants to understand how Azure can help prevent distributed denial of service (DDoS) and other attacks.

In this part, you learn how Azure DDoS Protection (Standard service tier) helps protect your Azure resources from DDoS attacks. First, let's define what a DDoS attack is.

What are DDoS attacks?

A distributed denial of service attack attempts to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users. DDoS attacks can target any resource that's publicly reachable through the internet, including websites.

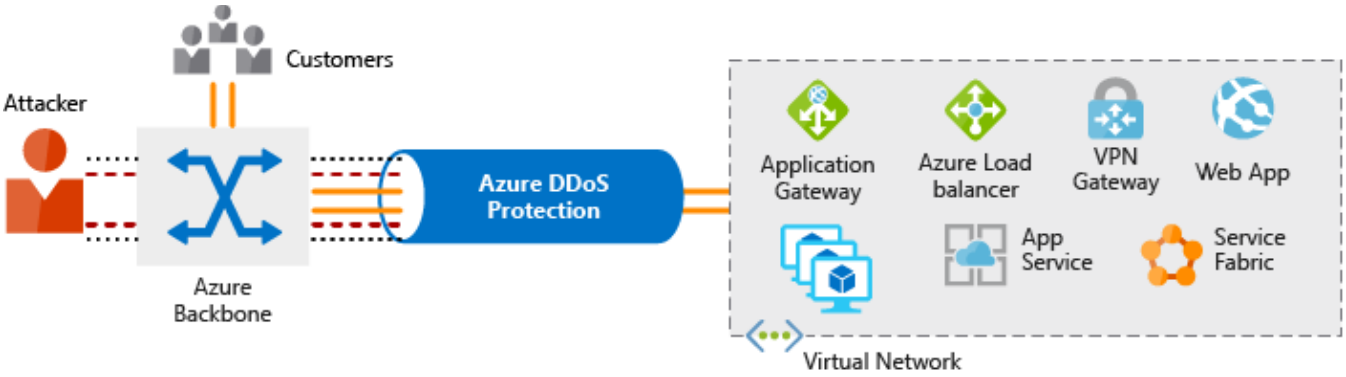
What is Azure DDoS Protection?

Azure DDoS Protection (Standard) helps protect your Azure resources from DDoS attacks.

When you combine DDoS Protection with recommended application design practices, you help provide a defense against DDoS attacks. DDoS Protection uses the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. The DDoS

Protection service helps protect your Azure applications by analyzing and discarding DDoS traffic at the Azure network edge, before it can affect your service's availability.

This diagram shows network traffic flowing into Azure from both customers and an attacker:



DDoS Protection identifies the attacker's attempt to overwhelm the network and blocks further traffic from them, ensuring that traffic never reaches Azure resources. Legitimate traffic from customers still flows into Azure without any interruption of service.

DDoS Protection can also help you manage your cloud consumption. When you run on-premises, you have a fixed number of compute resources. But in the cloud, elastic computing means that you can automatically scale out your deployment to meet demand. A cleverly designed DDoS attack can cause you to increase your resource allocation, which incurs unneeded expense. DDoS Protection Standard helps ensure that the network load you process reflects customer usage. You can also receive credit for any costs accrued for scaled-out resources during a DDoS attack.

What service tiers are available to DDoS Protection?

DDoS Protection provides these service tiers:

- **Basic**

  The Basic service tier is automatically enabled for free as part of your Azure subscription.

  Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. The Basic service tier ensures that Azure infrastructure itself is not affected during a large-scale DDoS attack.

  The Azure global network is used to distribute and mitigate attack traffic across Azure regions.

- **Standard**

The Standard service tier provides additional mitigation capabilities that are tuned specifically to Azure Virtual Network resources. DDoS Protection Standard is relatively easy to enable and requires no changes to your applications.

The Standard tier provides always-on traffic monitoring and real-time mitigation of common network-level attacks. It provides the same defenses that Microsoft's online services use.

Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses, which are associated with resources deployed in virtual networks such as Azure Load Balancer and Application Gateway.

The Azure global network is used to distribute and mitigate attack traffic across Azure regions.

What kinds of attacks can DDoS Protection help prevent?

The Standard service tier can help prevent:

- **Volumetric attacks**

  The goal of this attack is to flood the network layer with a substantial amount of seemingly legitimate traffic.

- **Protocol attacks**

  These attacks render a target inaccessible by exploiting a weakness in the layer 3 and layer 4 protocol stack.

- **Resource-layer (application-layer) attacks (only with web application firewall)**

  These attacks target web application packets to disrupt the transmission of data between hosts. You need a web application firewall (WAF) to protect against L7 attacks. DDoS Protection Standard protects the WAF from volumetric and protocol attacks.

Filter network traffic by using network security groups

Although Azure Firewall and Azure DDoS Protection can help control what traffic can come from outside sources, Tailwind Traders also wants to understand how to protect its internal networks on Azure. Doing so will give the company an extra layer of defense against attacks.

In this part, you examine network security groups (NSGs).

What are network security groups?

A network security group enables you to filter network traffic to and from Azure resources within an Azure virtual network. You can think of NSGs like an internal firewall. An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.

How do I specify NSG rules?

A network security group can contain as many rules as you need, within Azure subscription limits. Each rule specifies these properties:

Property	Description
Name	A unique name for the NSG.
Priority	A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers.
Source or Destination	A single IP address or IP address range, service tag, or application security group.
Protocol	**TCP**, **UDP**, or **Any**.
Direction	Whether the rule applies to inbound or outbound traffic.
Port Range	A single port or range of ports.
Action	**Allow** or **Deny**.

When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You can't remove the default rules, but you can override them by creating new rules with higher priorities.

Exercise - Configure network access to a VM by using a network security group

In this exercise, you configure network access to a virtual machine (VM) running on Azure.

You start by creating a Linux VM and installing Nginx, a popular web server, on that VM. To make your web server accessible, you then create a network security group (NSG) rule that allows inbound access on port 80 (HTTP).

There are many ways to create and manage VMs, including their network settings. For example, you can use the Azure portal, the Azure CLI, Azure PowerShell, or an Azure Resource Manager (ARM) template.

Here, you use the Azure CLI. The Azure CLI enables you to connect to Azure and run administrative commands on Azure resources. As with other command-line interfaces, you can run commands directly from a terminal or you can add commands to a Bash script or a PowerShell script. The Azure CLI runs on Windows, macOS, or Linux.

Here, you access the Azure CLI from Azure Cloud Shell. Cloud Shell is a browser-based shell experience that you use to manage and develop Azure resources. Think of Cloud Shell as an interactive console that runs in the cloud.

If you're new to the Azure CLI or to Cloud Shell, just follow along.

Create a Linux virtual machine and install Nginx

Use the following Azure CLI commands to create a Linux VM and install Nginx. After your VM is created, you'll use the Custom Script Extension to install Nginx. The Custom Script Extension is an easy way to download and run scripts on your Azure VMs. It's just one of the many ways you can configure the system after your VM is up and running.

1. From Cloud Shell, run the following `az vm create` command to create a Linux VM:

   Azure CLICopy

   ```
   az vm create \
     --resource-group [sandbox resource group name] \
     --name my-vm \
     --image UbuntuLTS \
     --admin-username azureuser \
     --generate-ssh-keys
   ```

   Your VM will take a few moments to come up.

   You name the VM **my-vm**. You use this name to refer to the VM in later steps.

2. Run the following `az vm extension set` command to configure Nginx on your VM:

   Azure CLICopy

   ```
   az vm extension set \
     --resource-group [sandbox resource group name] \
     --vm-name my-vm \
     --name customScript \
     --publisher Microsoft.Azure.Extensions \
     --version 2.1 \
     --settings
   '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-
   to-azure/master/configure-nginx.sh"]}' \
     --protected-settings '{"commandToExecute": "./configure-nginx.sh"}'
   ```

   This command uses the Custom Script Extension to run a Bash script on your VM. The script is stored on GitHub.

   While the command runs, you can choose to examine the Bash script from a separate browser tab.

   To summarize, the script:

1. Runs `apt-get update` to download the latest package information from the internet. This step helps ensure that the next command can locate the latest version of the Nginx package.
2. Installs Nginx.
3. Sets the home page, */var/www/html/index.html*, to print a welcome message that includes your VM's host name.

Access your web server

In this procedure, you get the IP address for your VM and attempt to access your web server's home page.

1. Run the following `az vm list-ip-addresses` command to get your VM's IP address and store the result as a Bash variable:

   Azure CLICopy

   ```
   IPADDRESS="$(az vm list-ip-addresses \
     --resource-group [sandbox resource group name] \
     --name my-vm \
     --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
     --output tsv)"
   ```

2. Run the following `curl` command to download the home page:

   BashCopy

   ```
   curl --connect-timeout 5 http://$IPADDRESS
   ```

   The `--connect-timeout` argument specifies to allow up to five seconds for the connection to occur.

   After five seconds, you see an error message that states that the connection timed out:

   OutputCopy

   ```
   curl: (28) Connection timed out after 5001 milliseconds
   ```

   This message means that the VM was not accessible within the timeout period.

3. As an optional step, try to access the web server from a browser:
   1. Run the following to print your VM's IP address to the console:

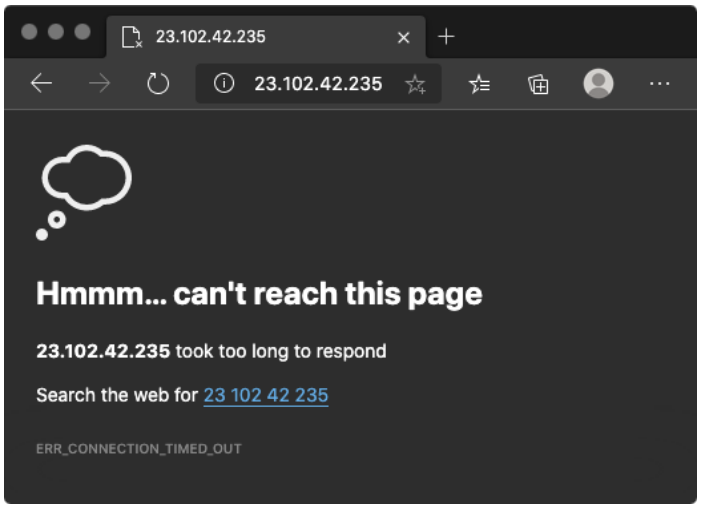
      BashCopy

      ```
      echo $IPADDRESS
      ```

      You see an IP address, for example, *23.102.42.235*.

   2. Copy the IP address that you see to the clipboard.
   3. Open a new browser tab and go to your web server.

After a few moments, you see that the connection isn't happening. If you wait for the browser to time out, you'll see something like this:



Keep this browser tab open for later.

List the current network security group rules

Your web server wasn't accessible. To find out why, let's examine your current NSG rules.

1. Run the following `az network nsg list` command to list the network security groups that are associated with your VM:

   Azure CLICopy

   ```
   az network nsg list \
     --resource-group [sandbox resource group name] \
     --query '[].name' \
     --output tsv
   ```

   You see this:

   OutputCopy

   ```
   my-vmNSG
   ```

   Every VM on Azure is associated with at least one network security group. In this case, Azure created an NSG for you called *my-vmNSG*.

2. Run the following `az network nsg rule list` command to list the rules associated with the NSG named *my-vmNSG*:

   Azure CLICopy

   ```
   az network nsg rule list \
     --resource-group [sandbox resource group name] \
     --nsg-name my-vmNSG
   ```

   You see a large block of text in JSON format in the output. In the next step, you'll run a similar command that makes this output easier to read.

3. Run the `az network nsg rule list` command a second time.

   This time, use the `--query` argument to retrieve only the name, priority, affected ports, and access (**Allow** or **Deny**) for each rule.

   The `--output` argument formats the output as a table so that it's easy to read.

Azure CLICopy

```
az network nsg rule list \
  --resource-group [sandbox resource group name] \
  --nsg-name my-vmNSG \
  --query    '[].{Name:name,    Priority:priority,    Port:destinationPortRange,
Access:access}' \
  --output table
```

You see this:

OutputCopy

```
Name               Priority    Port    Access
-----------------  ----------  ------  --------
default-allow-ssh  1000        22      Allow
```

You see the default rule, *default-allow-ssh*. This rule allows inbound connections over port 22 (SSH). SSH (Secure Shell) is a protocol that's used on Linux to allow administrators to access the system remotely.

The priority of this rule is 1000. Rules are processed in priority order, with lower numbers processed before higher numbers.

By default, a Linux VM's NSG allows network access only on port 22. This enables administrators to access the system. You need to also allow inbound connections on port 80, which allows access over HTTP.

Create the network security rule

Here, you create a network security rule that allows inbound access on port 80 (HTTP).

1. Run the following `az network nsg rule create` command to create a rule called *allow-http* that allows inbound access on port 80:

   Azure CLICopy

   ```
   az network nsg rule create \
     --resource-group [sandbox resource group name] \
     --nsg-name my-vmNSG \
     --name allow-http \
     --protocol tcp \
     --priority 100 \
     --destination-port-ranges 80 \
     --access Allow
   ```

   For learning purposes, here you set the priority to 100. In this case, the priority doesn't matter. You would need to consider the priority if you had overlapping port ranges.

2. To verify the configuration, run `az network nsg rule list` to see the updated list of rules:

Azure CLICopy

```
az network nsg rule list \
  --resource-group [sandbox resource group name] \
  --nsg-name my-vmNSG \
  --query    '[].{Name:name,    Priority:priority,    Port:destinationPortRange,
Access:access}' \
  --output table
```

You see this both the *default-allow-ssh* rule and your new rule, *allow-http*:

OutputCopy

```
Name               Priority    Port    Access
-----------------  ----------  ------  --------
default-allow-ssh  1000        22      Allow
allow-http         100         80      Allow
```

Access your web server again

Now that you've configured network access to port 80, let's try to access the web server a second time.

1. Run the same `curl` command that you ran earlier:

   BashCopy

   ```
   curl --connect-timeout 5 http://$IPADDRESS
   ```

   You see this:

   HTMLCopy

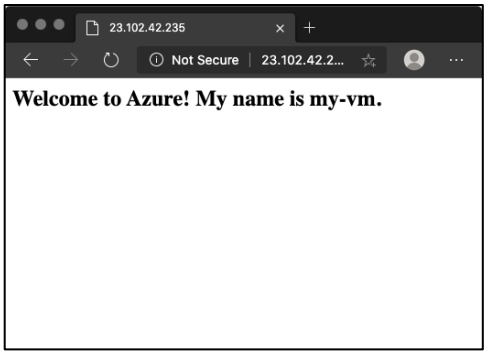
   ```
   <html><body><h2>Welcome to Azure! My name is my-vm.</h2></body></html>
   ```

   Note

   There may be a slight delay between rules being added and ports being opened.

2. As an optional step, refresh your browser tab that points to your web server.

   You see this:



Clean up

The sandbox automatically cleans up your resources when you're finished with this module.

When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

Nice work. In practice, you can create a standalone network security group that includes the inbound and outbound network access rules you need. If you have multiple VMs that serve the same purpose, you can assign that NSG to each VM at the time you create it. This technique enables you to control network access to multiple VMs under a single, central set of rules.

Combine Azure services to create a complete network security solution

When you're considering an Azure security solution, consider all the elements of defense in depth.

Here are some recommendations on how to combine Azure services to create a complete network security solution.

Secure the perimeter layer

The perimeter layer is about protecting your organization's resources from network-based attacks. Identifying these attacks, alerting the appropriate security teams, and eliminating their impact are important to keeping your network secure. To do this:

- Use Azure DDoS Protection to filter large-scale attacks before they can cause a denial of service for users.
- Use perimeter firewalls with Azure Firewall to identify and alert on malicious attacks against your network.

Secure the network layer

At this layer, the focus is on limiting network connectivity across all of your resources to allow only what's required. Segment your resources and use network-level controls to restrict communication to only what's needed.

By restricting connectivity, you reduce the risk of lateral movement throughout your network from an attack. Use network security groups to create rules that define allowed inbound and outbound communication at this layer. Here are some recommended practices:

- Limit communication between resources by segmenting your network and configuring access controls.
- Deny by default.
- Restrict inbound internet access and limit outbound where appropriate.
- Implement secure connectivity to on-premises networks.

Combine services

You can combine Azure networking and security services to manage your network security and provide increased layered protection. Here are two ways you can combine services:

- **Network security groups and Azure Firewall**

  Azure Firewall complements the functionality of network security groups. Together, they provide better defense-in-depth network security.

  Network security groups provide distributed network-layer traffic filtering to limit traffic to resources within virtual networks in each subscription.

  Azure Firewall is a fully stateful, centralized network firewall as a service. It provides network-level and application-level protection across different subscriptions and virtual networks.

- **Azure Application Gateway web application firewall and Azure Firewall**

  Web application firewall (WAF) is a feature of Azure Application Gateway that provides your web applications with centralized, inbound protection against common exploits and vulnerabilities.

  Azure Firewall provides:

  - Inbound protection for non-HTTP/S protocols (for example, RDP, SSH, and FTP).
  - Outbound network-level protection for all ports and protocols.
  - Application-level protection for outbound HTTP/S.

  Combining them provides more layers of protection.

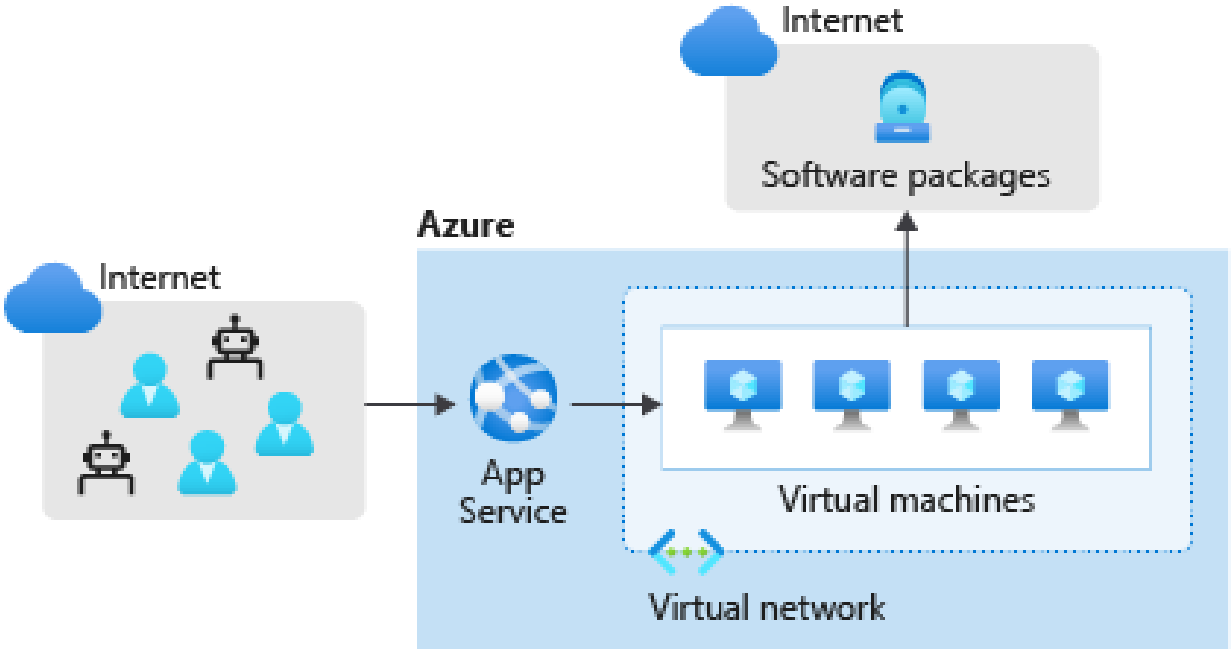
Knowledge check

Consider the following scenario. Then choose the best response for each question that follows and select **Check your answers**.

Tailwind Traders is moving its online payment system to Azure. The processing of online orders begins through a website, which Tailwind Traders manages through Azure App Service. (App Service is a way to host web applications on Azure.)

The web application that runs the website passes order information to virtual machines (VMs), which further process each order. These VMs exist on an Azure virtual network, but they need to access the internet to retrieve software packages and system updates.

Here's a diagram that shows the basic architecture of the company's payment system:



The security team wants to ensure that only valid network traffic reaches the company's Azure resources. As an extra layer of defense, the team also wants to ensure that the VMs can reach only trusted hosts on specific ports.

Check your knowledge

1. An attacker can bring down your website by sending a large volume of network traffic to your servers. Which Azure service can help Tailwind Traders protect its App Service instance from this kind of attack?

- Azure Firewall
- Network security groups
- Azure DDoS Protection

2. What's the best way for Tailwind Traders to limit all outbound traffic from VMs to known hosts?

- Configure Azure DDoS Protection to limit network access to trusted ports and hosts.
- Create application rules in Azure Firewall.
- Ensure that all running applications communicate with only trusted ports and hosts.

3. How can Tailwind Traders most easily implement a *deny by default* policy so that VMs can't connect to each other?

- Allocate each VM on its own virtual network.
- Create a network security group rule that prevents access from another VM on the same network.
- Configure Azure DDoS Protection to limit network access within the virtual network.