

Configure network security groups

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/configure-network-security-groups/1-introduction>

Introduction

Completed

Network security groups are a way to limit network traffic to resources in your virtual network. Network security groups contain a list of security rules that allow or deny inbound or outbound network traffic.

Suppose your company has several locations and wants to migrate to a cloud based solution. The company only considers moving key systems onto the cloud platform if stringent security requirements can be met. These requirements include tight control over which computers have network access to the app servers. You need to secure both virtual machine networking and Azure services networking. Your goal is to prevent unwanted or unsecured network traffic from being able to reach key systems.

In this module, you learn how to create an AI-ready network security group, configure inbound and outbound port rules, and verify secure connectivity. The goal of this module is to teach you how to control network traffic with network security groups.

Learning objectives

In this module, you learn how to:

- Determine when to use network security groups.
- Create network security groups.
- Implement and evaluate network security group rules.
- Describe the function of application security groups.

Skills measured

The content in the module helps you prepare for [Exam AZ-104: Microsoft Azure Administrator](#).

Prerequisites

- Familiarity with Azure virtual networks and resources such as virtual machines.
- Working knowledge of the Azure portal so you can configure the network security groups.
- Basic understanding of traffic routing and traffic control strategies.

2. Implement network security groups

<https://learn.microsoft.com/en-us/training/modules/configure-network-security-groups/2-implement-network-security-groups>

Implement network security groups

Completed

You can limit network traffic to resources in your virtual network by using a [network security group](#). You can assign a network security group to a subnet or a network interface, and define security rules in the group to control network traffic.

Things to know about network security groups

Let's look at the characteristics of network security groups.

- A network security group contains a list of security rules that allow or deny inbound or outbound network traffic.
- A network security group can be associated to a subnet or a network interface.
- A network security group can be associated multiple times.
- You create a network security group and define security rules in the Azure portal.
- The Overview page for a virtual machine provides information about the associated network security groups. You can see details such as the assigned subnets, assigned network interfaces,

and the defined security rules.

Network security group: nsg0 | Directory: Microsoft

Search (Ctrl+/) << >> Move Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource group (change) : rg01

Location : East US

Subscription (change) :

Subscription ID :

Tags (change) : [Click here to add tags](#)

Custom security rules : 1 inbound, 0 outbound

Associated with : 1 subnets, 0 network interfaces

Network security groups and subnets

You can assign network security groups to a subnet and create a protected screened subnet (also referred to as a demilitarized zone or *DMZ*). A DMZ acts as a buffer between resources within your virtual network and the internet.

- Use the network security group to restrict traffic flow to all machines that reside within the subnet.
- Each subnet can have a maximum of one associated network security group.

Network security groups and network interfaces

You can assign network security groups to a network interface card (NIC).

- Define network security group rules to control all traffic that flows through a network interface.
- Each network interface that exists in a subnet can have zero, or one, associated network security groups.

3. Determine network security group rules

<https://learn.microsoft.com/en-us/training/modules/configure-network-security-groups/3-determine-network-security-groups-rules>

Determine network security group rules

Completed

Security rules in network security groups enable you to filter network traffic. You can define rules to control the traffic flow in and out of virtual network subnets and network interfaces.

Things to know about security rules

Let's review the characteristics of security rules in network security groups.

- Azure creates several default security rules within each network security group, including inbound traffic and outbound traffic. Examples of default rules include `DenyAllInbound` traffic and `AllowInternetOutbound` traffic.
- Azure creates the default security rules in each network security group that you create.
- You can add more security rules to a network security group by [specifying conditions](#). Here's a list of the most common conditions.

Setting	Value
Source	Any, IP Addresses, My IP address, Service Tag, or Application security group
Source port ranges	Specify the ports on which the rule allows or denies traffic
Destination	Any, IP Addresses, Service Tag, or Application security group
Protocol	Restrict the rule to Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Encapsulating Security Payload (ESP), or Authentication Header (AH). ESP and AH protocols are only available via JSON templates and PowerShell. The default is for the rule to apply to all protocols (Any).
Action	Allow or Deny
Priority	A value between 100 and 4,096 that's unique for all security rules within the NSG

- Each security rule is assigned a Priority value. All security rules for a network security group are processed in priority order. When a rule has a low Priority value, the rule has a higher priority or precedence in terms of order processing.
- You can't remove the default security rules.
- You can override a default security rule by creating another security rule that has a higher Priority setting for your network security group.

Inbound traffic rules

Azure defines three default inbound security rules for your network security group. These rules **deny all inbound traffic** except traffic from your virtual network and Azure load balancers. The next image shows the default inbound security rules for a network security group in the Azure portal.

VM1-nsg - Inbound security rules

Network security group

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Outbound traffic rules

Azure defines three default outbound security rules for your network security group. These rules **only allow outbound traffic** to the internet and your virtual network. The next image shows the default outbound security rules for a network security group in the Azure portal.

VM1-nsg - Outbound security rules

Network security group

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

4. Determine network security group effective rules

<https://learn.microsoft.com/en-us/training/modules/configure-network-security-groups/4-determine-network-security-groups-effective-rules>

Determine network security group effective rules

Completed

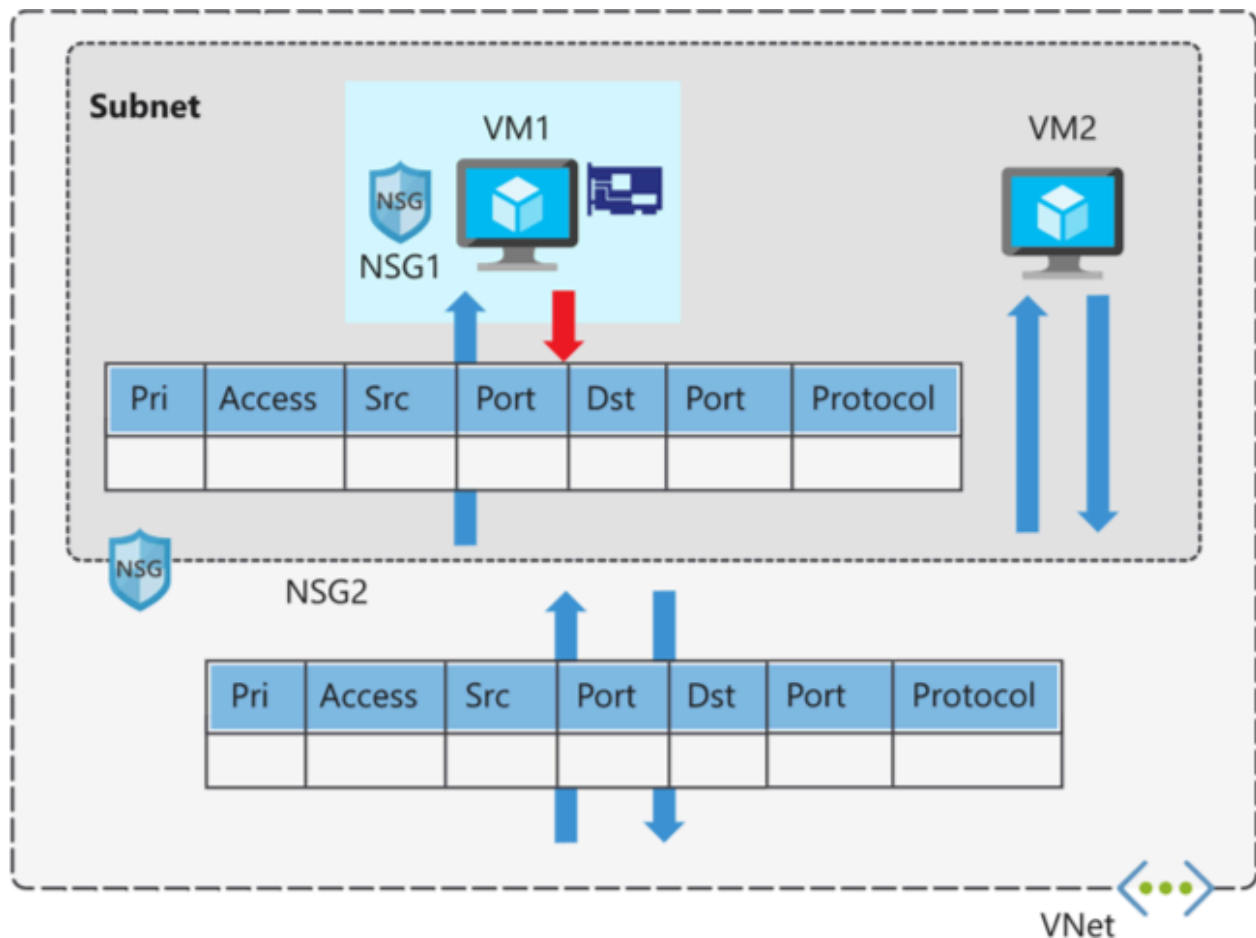
Each network security group and its defined security rules are evaluated independently. Azure processes the conditions in each rule defined for each virtual machine in your configuration.

- For inbound traffic, Azure first processes network security group security rules for any associated subnets and then any associated network interfaces.
- For outbound traffic, the process is reversed. Azure first evaluates network security group security rules for any associated network interfaces followed by any associated subnets.
- For both the inbound and outbound evaluation process, Azure also checks how to apply the rules for intra-subnet traffic. Intra-subnet traffic refers to virtual machines in the same subnet.

How Azure ends up applying your defined security rules for a virtual machine determines the overall *effectiveness* of your rules.

Network security group evaluation

When you apply network security groups to both a subnet and a network interface, each network security group is evaluated independently. Both inbound and outbound rules are considered based on the priority and processing order.



Things to consider when creating effective rules

Review the following considerations regarding creating effective security rules for machines in your virtual network.

- **Consider allowing all traffic.** If you place your virtual machine within a subnet or utilize a network interface, you don't have to associate the subnet or NIC with a network security group. This approach allows all network traffic through the subnet or NIC according to the default Azure security rules. If you're not concerned about controlling traffic to your resource at a specific level, then don't associate your resource at that level to a network security group.
- **Consider importance of allow rules.** When you create a network security group, you must define an **allow** rule for both the subnet and network interface in the group to ensure traffic can get through. If you have a subnet or NIC in your network security group, you must define an allow rule at each level. Otherwise, the traffic is denied for any level that doesn't provide an allow rule definition.
- **Consider intra-subnet traffic.** The security rules for a network security group associated to a subnet can affect traffic between all virtual machines in the subnet. You can prohibit intra-subnet traffic by defining a rule in the network security group to deny all inbound and outbound traffic. This rule prevents all virtual machines in your subnet from communicating with each other.

- **Consider rule priority.** The security rules for a network security group are processed in priority order. To ensure a particular security rule is always processed, assign the lowest possible priority value to the rule. It's a good practice to leave gaps in your priority numbering, such as 100, 200, 300, and so. The gaps in the numbering allow you to add new rules without having to edit existing rules.

View effective security rules

If you have several network security groups and aren't sure which security rules are being applied, you can use the **Effective security rules** link in the Azure portal. You can use the link to verify which security rules are applied to your machines, subnets, and network interfaces.

The screenshot shows the 'Effective security rules' page in the Azure portal for a network security group named 'nsgtest'. The page has a left-hand navigation pane with options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Monitoring, Automation, and Help. The 'Effective security rules' option is highlighted. The main content area has a search bar, 'Download' and 'Refresh' buttons, and a message: 'Select a network interface below to see the effective security rules and network security groups associated with it.' Below this, there are dropdown menus for 'Scope' (set to 'Network security group (nsgtest)'), 'Virtual machine', and 'Network interface'. At the bottom, it shows 'Associated NSGs: 1 None'.

Note

[Network Watcher](#) provides a consolidated view of your infrastructure rules, including both NSG rules and Azure Virtual Network Manager security admin rules. The IP flow verify feature evaluates traffic against both NSG rules and any security admin rules that may be in effect.

5. Create network security group rules

<https://learn.microsoft.com/en-us/training/modules/configure-network-security-groups/5-create-network-security-groups-rules>

Create network security group rules

Completed

It's easy to add security rules to control inbound and outbound traffic in the Azure portal. You can configure your virtual network security group rule settings, and select from a large variety of communication services, including HTTPS, RDP, FTP, and DNS.

Things to know about configuring security rules

Let's look at some of the properties you need to specify to create your security rules. As you review these settings, think about the traffic rules you need to create and what services can fulfill your network requirements.

Source ⓘ

Source port ranges * ⓘ

Destination ⓘ

Service ⓘ

Destination port ranges * ⓘ

- **Source:** Identifies how the security rule controls **inbound** traffic. The value specifies a specific source IP address range to allow or deny. The source filter can be any resource, an IP address range, an application security group, or a default tag.
- **Destination:** Identifies how the security rule controls **outbound** traffic. The value specifies a specific destination IP address range to allow or deny. The destination filter value is similar to the source filter. The value can be any resource, an IP address range, an application security group, or a default tag.
- **Service:** Specifies the destination protocol and port range for the security rule. You can choose a predefined service like RDP or SSH or provide a custom port range. There are a large number of services to select from.

Service ⓘ

Custom

SSH

RDP

Custom

FTP

- **Priority:** Assigns the priority order value for the security rule. Rules are processed according to the priority order of all rules for a network security group, including a subnet and network interface. The lower the priority value, the higher priority for the rule.

Priority * ⓘ

119 ✓

Name *

AllowAnyCustom8080Inbound

When to use augmented security rules

A single network security group rule can contain multiple values in the Source, Destination, and Service fields. This approach, called augmented security rules, reduces the total number of rules needed and simplifies NSG management.

Things to know about augmented security rules

- **Multiple IP addresses:** Combine multiple IP addresses into one rule.
- **Multiple port ranges:** Specify multiple ports and ranges in the Service field.
- **Service tags and ASGs:** Mix service tags, application security groups, and IP addresses within the same rule.
- **Reduced rule count:** Instead of creating separate rules for each IP range or port, combine them into fewer, more manageable rules.

In enterprise environments with many IP ranges or services, augmented rules prevent NSG rule sprawl. For example, instead of creating four separate rules for ports 80, 443, 8080, and 8090, create one rule with all the ports.

Tip

Expand your learning with the [Secure and isolate access to Azure resources by using network security groups and service endpoints](#) training module. This module includes a sandbox where you can practice.

6. Implement application security groups

<https://learn.microsoft.com/en-us/training/modules/configure-network-security-groups/6-implement-asgs>

Implement application security groups

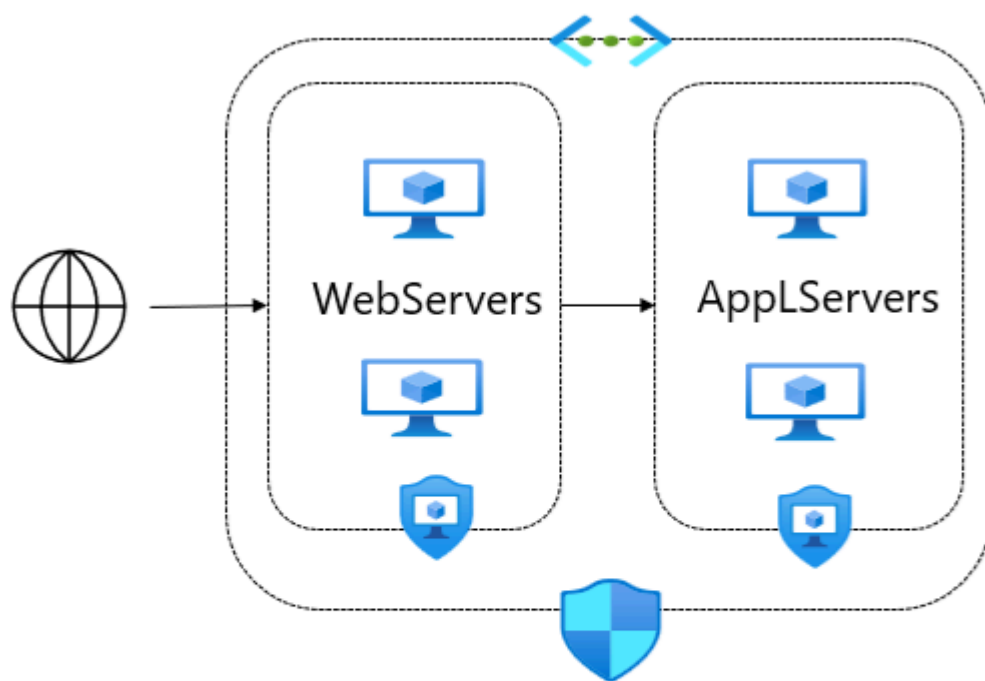
Completed

You can implement [application security groups \(ASGs\)](#) in your Azure virtual network to logically group your virtual machines by workload. You can then define your network security group rules based on your application security groups.

Things to know about using application security groups

Application security groups provide an application-centric way of looking at your infrastructure. You join your virtual machines to an application security group. Then you use the application security group as a source or destination in the network security group rules.

Let's examine how to implement application security groups by creating a configuration for an online retailer. In our example scenario, we need to control network traffic to virtual machines in application security groups.



Source	Destination	Port
Internet	WebServers	80, 443
WebServers	SQLServers	1433

Note

In the diagram, the application servers are handing SQL Server requests.

Scenario requirements

Here are the scenario requirements for our example configuration:

- In this scenario, there are two tiers: web servers and application servers.
- The web servers handle HTTP and HTTPS internet traffic.
- The application servers process SQL requests from the web servers.

Solution

For our scenario, we need to build the following configuration:

1. Create application security groups for each tier.
2. For each virtual machine server, assign its network interface to the appropriate application security group.
3. Create the network security group and security rules.

- **Rule 1:** Set **Priority** to 100. Allow access from the internet to the web servers machines from HTTP port 80 and HTTPS port 443.

Rule 1 has the lowest priority value, so it has precedence over the other rules in the group. Customer access to our online catalog is paramount in our design.

- **Rule 2:** Set **Priority** to 110. Allow access from the web servers to application servers over SQL port 1433.
- **Rule 3:** Set **Priority** to 120. **Deny** access from anywhere to application server machines on the HTTP and HTTPS ports.

The combination of Rule 2 and Rule 3 ensures that only our web servers can access our database servers. This security configuration protects our inventory databases from outside attack.

Things to consider when using application security groups

There are several advantages to implementing application security groups in your virtual networks.

- **Consider IP address maintenance.** When you control network traffic by using application security groups, you don't need to configure inbound and outbound traffic for specific IP addresses. If you have many virtual machines in your configuration, it can be difficult to specify all of the affected IP addresses. As you maintain your configuration, the number of your servers can change. These changes can require you to modify how you support different IP addresses in your security rules.
- **Consider no subnets.** By organizing your virtual machines into application security groups, you don't need to also distribute your servers across specific subnets. You can arrange your servers by application and purpose to achieve logical groupings.
- **Consider simplified rules.** Application security groups help to eliminate the need for multiple rule sets. You don't need to create a separate rule for each virtual machine. You can dynamically apply new rules to designated application security groups. New security rules are automatically applied to all the virtual machines in the specified application security group.
- **Consider workload support.** A configuration that implements application security groups is easy to maintain and understand because the organization is based on workload usage. Application security groups provide logical arrangements for your applications, services, data storage, and workloads.
- **Consider service tags.** Service Tags represent a group of IP address prefixes from a specific Azure service. They help minimize the complexity of frequent updates on network security rules. While service tags are used to simplify the management of IP addresses for Azure services, ASGs are used to group VMs and manage network security policies based on those groups.

7. Exercise - Implement virtual networking

<https://learn.microsoft.com/en-us/training/modules/configure-network-security-groups/7-simulation-create-net-work-groups>

Exercise - Implement virtual networking

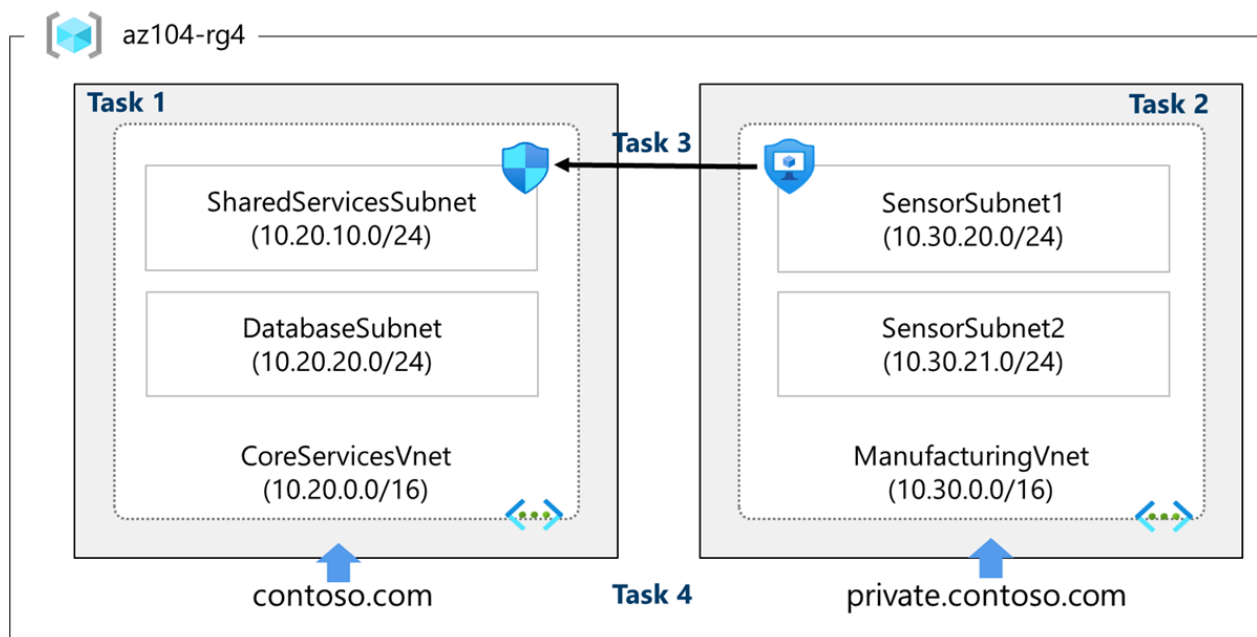
Completed

Lab scenario

Your organization wants to ensure that access to virtual machines is restricted. As the Azure Administrator, you need to:

- Create and configure network security groups.
- Associate network security groups to virtual machines.
- Deny and allow access to the virtual machines by using network security groups.

Architecture diagram



Job skills

- Create a virtual network with subnets using the portal.

- Create a virtual network and subnets using a template.
- Create and configure communication between an Application Security Group and a Network Security Group.
- Configure public and private Azure DNS zones. (optional)

Important

Estimated time: 50 minutes. To complete this exercise, you need an [Azure subscription](#).

Launch the exercise, and follow the instructions. When finished, be sure to return to this page so you can continue learning.

[Launch Exercise](#)

8. Module assessment

<https://learn.microsoft.com/en-us/training/modules/configure-network-security-groups/8-knowledge-check>

Module assessment

Completed

9. Summary and resources

<https://learn.microsoft.com/en-us/training/modules/configure-network-security-groups/9-summary-resources>

Summary and resources

Completed

In this module, you learned about network security groups (NSGs) in Azure. NSGs are used to limit network traffic to resources in your virtual network by containing a list of security rules. You can associate NSGs with subnets or network interfaces and define rules to control inbound and outbound traffic.

You also learned how NSG rules are evaluated and processed. Lastly, you learned how application security groups, allow for grouping virtual machines based on workload.

The main takeaways from this module are:

- Network security groups are essential for controlling network traffic in Azure virtual networks.
- NSG rules are evaluated and processed based on priority and can be created for subnets and network interfaces.
- Effective NSG rules can be achieved by considering rule precedence, intra-subnet traffic, and managing rule priority.
- Application security groups provide an application-centric view of infrastructure and simplify rule management.

Learn more with Copilot

Copilot can assist you in designing Azure infrastructure solutions. Copilot can compare, recommend, explain, and research products and services where you need more information. Open a Microsoft Edge browser and choose Copilot (top right) or navigate to copilot.microsoft.com. Take a few minutes to try these prompts and extend your learning with Copilot.

- What is the difference between an Azure network security group and an application security group? Provide usage examples.
- Can you explain NSG rules in detail?
- How can I troubleshoot network security group rules?

Learn more with documentation

- [Read about network security groups](#). This article describes the properties of a network security group rule, the default security rules that are applied, and the rule properties that you can modify.
- [Filter network traffic with network security groups in the Azure portal](#). Learn how to create a network security group and an application security group.
- [Create, change, or delete a network security group](#). Learn how to work with network and application security groups.
- [Application security groups](#). Learn about application security groups and traffic control with rules.

Learn more with self-paced training

- [Secure and isolate access to Azure resources with network security groups and service endpoints \(sandbox\)](#). Learn how to secure your virtual machines and Azure services from unauthorized network access.
- [Filter network traffic with a network security group using the Azure portal](#). Learn how to create, configure, and apply NSGs for improved network security.