Network security groups

Friday, October 18, 2024

03:45

You can use an Azure network security group to filter network traffic between Azure resources in an Azure virtual network.

A network security group contains [security rules](https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

Security rules

A network security group contains as many rules as desired, within Azure subscription [limits](https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits?toc=/azure/virtual-network/toc.json#azure-resource-manager-virtual-networking-limits). Each rule specifies the following properties:

|  |  |
| --- | --- |
| **Property** | **Explanation** |
| Name | A unique name within the network security group. The name can be up to 80 characters long. It must begin with a word character, and it must end with a word character or with '\_'. The name may contain word characters or '.', '-', '\_'. |
| Priority | A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities aren't processed.  Azure default security rules are given the highest number with the lowest priority to ensure that custom rules are always processed first. |
| Source or destination | Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or application security group.  If you specify an address for an Azure resource, specify the private IP address assigned to the resource.  Network security groups are processed after Azure translates a public IP address to a private IP address for inbound traffic, and before Azure translates a private IP address to a public IP address for outbound traffic.  If source points to the subnet 10.0.1.0/24 (where VM1 is located) and destination points to the subnet 10.0.2.0/24 (where VM2 is located), this indicates the purpose of NSG is to filter network traffic for VM2 and the NSG is associated with the network interface of VM2. |
| Protocol | TCP, UDP, ICMP, ESP, AH, or Any. The ESP and AH protocols aren't currently available via the Azure portal but can be used via ARM templates. |
| Direction | Whether the rule applies to inbound, or outbound traffic. |
| Port range | You can specify an individual or range of ports. For example, you could specify 80 or 10000-10005. Specifying ranges enables you to create fewer security rules. |
| Action | Allow or deny |
|  |  |

Security rules are evaluated and applied based on the five-tuple (source, source port, destination, destination port, and protocol) information.

You can't create two security rules with the same priority and direction.

A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record.

The flow record allows a network security group to be stateful.

If you specify an outbound security rule to any address over port 80, for example, it's not necessary to specify an inbound security rule for the response to the outbound traffic. You only need to specify an inbound security rule if communication is initiated externally.

The opposite is also true. If inbound traffic is allowed over a port, it's not necessary to specify an outbound security rule to respond to traffic over the port.

Existing connections may not be interrupted when you remove a security rule that allowed the connection. Modifying network security group rules will only affect new connections. When a new rule is created or an existing rule is updated in a network security group, it will only apply to new connections. Existing connections are not reevaluated with the new rules.

There are limits to the number of security rules you can create in a network security group. For details, see [Azure limits](https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits?toc=/azure/virtual-network/toc.json#azure-resource-manager-virtual-networking-limits).

Default security rules

Azure creates the following default rules in each network security group that you create:

Inbound

AllowVNetInBound

Expand table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | Any | Allow |

AllowAzureLoadBalancerInBound

Expand table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65001 | AzureLoadBalancer | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Allow |

DenyAllInbound

Expand table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Deny |

Outbound

AllowVnetOutBound

Expand table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | Any | Allow |

AllowInternetOutBound

Expand table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65001 | 0.0.0.0/0 | 0-65535 | Internet | 0-65535 | Any | Allow |

DenyAllOutBound

Expand table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Deny |

You can't remove the default rules, but you can override them by creating rules with higher priorities.