Configuring Azure Security Groups in Cisco Nexus Dashboard Orchestrator

Revised: February 19, 2022,

New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior

Feature or Change	Description	Where Documented
Initial release of document	Initial release of document.	

Security Groups

Note The following content refers to "Multi-Site Orchestrator" which has been rebranded to Nexus Dashboard Orchestrator. Same information is applicable to both products

In Azure, two types of security groups are used to administer and control network traffic within a virtual network (VNet):

- Network security groups: Network security groups, or NSGs, are used in Azure to filter network traffic to and from Azure resources. An NSG is used to define incoming and outgoing security policies, and contains 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.

  In Cloud APIC, an NSG is automatically configured based on a contract.

- Application security groups: Application security groups, or ASGs, are used in Azure to group virtual machine (VM) NICs according to the applications that run on them and define network security policies based on those groups. ASGs are used within an NSG to define these security polices and to apply a network security rule to a specific workload or group of virtual machines.

  In Cloud APIC, an ASG is a collection of endpoints for each EPG and is referenced as the source or destination in the NSG security policies.

The way that these security groups are configured, and what they are mapped to, differ depending on the release.

- Releases Prior to Release 5.1(2): NSG-Per-EPG Configurations, on page 2
- Release 5.1(2) and Later: NSG-Per-Subnet Configurations, on page 3

Releases Prior to Release 5.1(2): NSG-Per-EPG Configurations

For releases prior to Release 5.1(2), there is a one-to-one mapping between NSGs in Azure and EPGs on Cloud APIC (these configurations are also referred to as NSG-per-EPG configurations throughout this document). These NSGs for the Cloud APIC EPGs are populated with security rules based on contracts associated with the EPGs.

For releases prior to Release 5.1(2), the creation of an EPG in Cloud APIC results in the creation of the following Azure components:

- An ASG, which is used to group all endpoints or virtual machine NICs for each EPG based on the endpoint selectors
- An NSG, which gets associated with all of the NICs in that ASG and provides the security policy definition for that EPG

Release 5.1(2) and Later: NSG-Per-Subnet Configurations

Beginning with Release 5.1(2), in addition to the existing NSG-per-EPG configurations available previously, NSGs in Azure can also have a one-to-one mapping with subnets rather than EPGs on Cloud APIC (these configurations are also referred to as NSG-per-subnet configurations throughout this document). By default, NSGs are no longer created for EPGs beginning with Release 5.1(2), and NSGs are no longer associated with the endpoints and VM NICs in the ASG for that EPG. Instead, the NSG for each subnet will contain all of the rules based on the contracts for the ASGs, which have their endpoints discovered in the subnet.

For NSG-per-subnet configurations, the creation of an EPG in Cloud APIC results in the creation of the following Azure components:

- An ASG, which is used to group all endpoints or virtual machine NICs for each EPG based on the endpoint selectors [essentially no change in behavior for ASGs from releases prior to Release 5.1(2)]
- An NSG, which continues to provide the security policy definition for that EPG, but now gets associated with a subnet in a Cloud APIC-managed VNet

Looked at from another perspective:

- Every EPG in a Cloud APIC-managed VNet will have an ASG associated with it, which will group all the endpoints based on the endpoint selectors configured for the EPG.
- Every subnet in a Cloud APIC-managed VNet will have an NSG associated with it.

The default setting for a Greenfield or a fresh Cloud APIC deployment is NSG-per-subnet. When manually setting this configuration, as described previously, you can choose either a newer NSG-per-subnet configuration or the older NSG-per-EPG configuration beginning with Release 5.1(2). However, we recommend choosing the newer NSG-per-subnet configuration for several reasons:

- Using the NSG-per-subnet configuration reduces the number of NSGs in the VNet, and also reduces the number of rules for deployments with a large number of subnets accessing common shared services. This provides for easier management, since all of the rules can be checked in one NSG for a subnet, rather than for each NSG mapped to individual EPGs or ASGs.
- You must use the NSG-per-subnet configuration if you are configuring service EPGs. See the Cisco Cloud APIC for Azure User Guide, Release 5.1(x) or later, in the Cisco Cloud APIC documentation library for more information.

See the Cisco Cloud APIC for Azure User Guide, Release 5.1(x) or later, in the Cisco Cloud APIC documentation library for instructions on enabling or disabling the NSG-per-EPG or NSG-per-subnet configurations.

Guidelines and Limitations for ASGs and NSGs

Following are the guidelines and limitations for ASGs and NSGs.

- Guidelines and Limitations for Releases Prior to 5.1(2), on page 3
- Guidelines and Limitations for Release 5.1(2) or Later, on page 3

Guidelines and Limitations for Releases Prior to 5.1(2)

For releases prior to Release 5.1(2), support is only available for NSG-to-EPG mapping for Cloud APIC.

Guidelines and Limitations for Release 5.1(2) or Later

- Beginning with Release 5.1(2), support is also available for NSG-to-subnet mapping for Cloud APIC. However, you can have either the newer NSG-per-subnet configuration or the NSG-per-EPG configuration, but not both in the same Cloud APIC system.

- You can configure one NSG per subnet in a Cloud APIC-managed VNET. Having one NSG per a group of subnets is not supported for Cloud APIC at this time.
- Passthrough devices, such as transparent firewall, will not have NSGs attached to their NICs. If there are multiple passthrough devices sharing a subnet, the passthrough rules for each device will apply to all endpoints in the subnet.

Security Rules

The security rules for NSG differ, depending on whether they are rules for NSG-per-EPG configurations or for NSG-per-subnet configurations. A major distinction on the processing of the security rules between the two types of configurations is the trigger for installing and deleting the rules.

- NSG-Per-EPG Security Rules, on page 4
- NSG-Per-Subnet Security Rules, on page 4

NSG-Per-EPG Security Rules

- Once the EPGs and the contract are defined on the Cloud APIC, the NSG security rules that use ASGs as the source and destination are always programmed, regardless of whether an endpoint for the ASG that is referenced in the NSG security rule is discovered or not.
- For inter-VRF contracts:
  - If either the consumer or the provider EPG uses an endpoint selector based on subnet, then the NSG security rules that have the source or destination as the subnet from the EPG selector are always programmed, regardless of the discovery of an endpoint.
  - If the consumer or provider EPG does not use an endpoint selector based on subnet, then the NSG security rules using the endpoint's IP address as the source and destination are programmed, depending on the discovery of an endpoint.
- The rules created for an inter-site contract, where a cloud external EPG (`cloudExtEPg`) is involved, also get pre-programmed without the endpoint getting discovered.

NSG-Per-Subnet Security Rules

The NSG security rules for an EPG are not programmed in a subnet-based NSG until the EPG has at least one endpoint discovered in that subnet.

Configuring Network Security Groups

Procedure

Step 1 In ACI Multi-Site Orchestrator, navigate to Application Management > Policies.

The Policies window appears.

Step 2 Click Add Policy, then choose Network Security Group Policy from the pull-down menu.

The Add Network Security Group Policy window appears.

Step 3 Enter a name for the network security group policy.

If you enter a name that is being used already, you will get an error message. Enter a different, unused name for the network security group to clear the error message.

Step 4 Determine the current setting for the Network Security Group at Subnet Level field.

- If you see a check in the box underneath the Network Security Group at Subnet Level field, that means that you have the newer NSG-per-subnet configuration.
- If you do not see a check in the box underneath the Network Security Group at Subnet Level field (if the box is empty), that means that you have the older NSG-per-EPG configuration.

Step 5 Determine if you want to change the setting for the Network Security Group at Subnet Level field or leave it as-is.

Desired Configuration	Existing Configuration	Action
If you want to have the newer NSG-per-subnet configuration, and:	You see a check in the box underneath the Network Security Group at Subnet Level field, then:	You are already set up with the NSG-per-subnet configuration that you want. You do not have to make any changes.
	You do not see a check in the box underneath the Network Security Group at Subnet Level field, then:	You will have to change the setting in the Network Security Group at Subnet Level field. Go to Step 6, on page 5.
If you want to have the older NSG-per-EPG configuration, and:	You see a check in the box underneath the Network Security Group at Subnet Level field, then:	You will have to change the setting in the Network Security Group at Subnet Level field. Go to Step 6, on page 5.
	You do not see a check in the box underneath the Network Security Group at Subnet Level field, then:	You are already set up with the NSG-per-EPG configuration that you want. You do not have to make any changes.

Step 6 Make the necessary changes in this window.

Note Changing the network security group setting will result in traffic loss. If you have to change the network security group setting, we recommend that you make the change during a maintenance window.

- If you want to have the newer NSG-per-subnet configuration and you do not see a check in the box underneath the Network Security Group at Subnet Level field, click the box to add the check mark to enable the newer NSG-per-subnet configuration.
- If you want to have the older NSG-per-EPG configuration and you see a check in the box underneath the Network Security Group at Subnet Level field, then click the box to remove the check mark. This allows you to disable the newer NSG-per-subnet configuration, and to enable the older NSG-per-EPG configuration.

  Note the following:

  - Changing the setting from the newer NSG-per-subnet to the older NSG-per-EPG configuration is not recommended. Disabling the NSG-per-subnet setting means losing support for service EPG configurations and will result in traffic loss.

- If you have a service EPG or a private link label configured, you will not be able to disable the NSG-per-subnet configuration. You must disable the configured service EPG and/or a private link label before you can disable the NSG-per-subnet configuration.

Step 7 Select the Azure sites that you want to have associated with this configuration.

Click the box next to Azure Sites to select or deselect all of the Azure sites in the list.

If you do not select any Azure sites in this area, you can still save this network security group policy and then return to this policy at a later date to add the necessary Azure sites at that time.

Step 8 Click Save after you have made the necessary changes in the Add Network Security Group Policy window.

The Policies window appears again, with the new network security group policy listed.

- To edit a network security group policy, right-click on … in the far right area on the row for that network security group policy and select Edit.
- To delete a network security group policy, right-click on … in the far right area on the row for that network security group policy and select Delete, then click Yes in the confirmation window.

  If there are Azure sites associated with the network security group policy, you will see an error saying that the policy cannot be deleted because it is being used by one or more sites. Click on the link for the policy in that case, click the box next to Azure Sites to deselect all of the Azure sites that are selected in the list for this policy, and then click Save.

Trademarks

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.