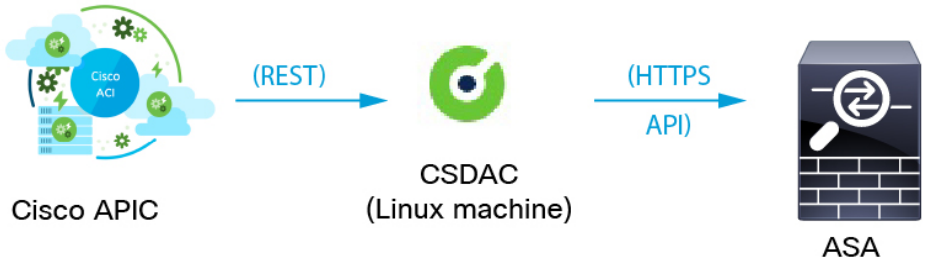
About the Cisco APIC Integration with ASA

This chapter discusses the integration between Cisco Application Policy Infrastructure Controller (APIC) and ASA.

About the Cisco APIC Integration with ASA

The dynamic attributes connector enables you to send Cisco APIC dynamic endpoint group (EPG) and endpoint security group (ESG) data from Cisco APIC tenants to an ASA. The following figure shows how this works at a high level.



Cisco APIC defines endpoint groups (EPGs) and endpoint security groups (ESGs) that have network object groups. Create a connector in the dynamic attributes connector that pulls that data from Cisco APIC tenants to ASA on which you can use those objects in access control rules. An ASA adapter pushes network object groups in the configured security context.

(You have the option to specify the tenants from which retrieve EPG and ESG objects when you set up the ASA adapter in the dynamic attributes connector. The Cisco APIC user determines which tenants data can be pulled from.)

You can optionally create an empty network object in the ASA CLI under which to create additional network objects sent from Cisco APIC. For more information, see Access Control Lists.

Note ASDM does not support creating empty network objects at this time.

About the Cisco APIC Integration with ASA

Sample configuration

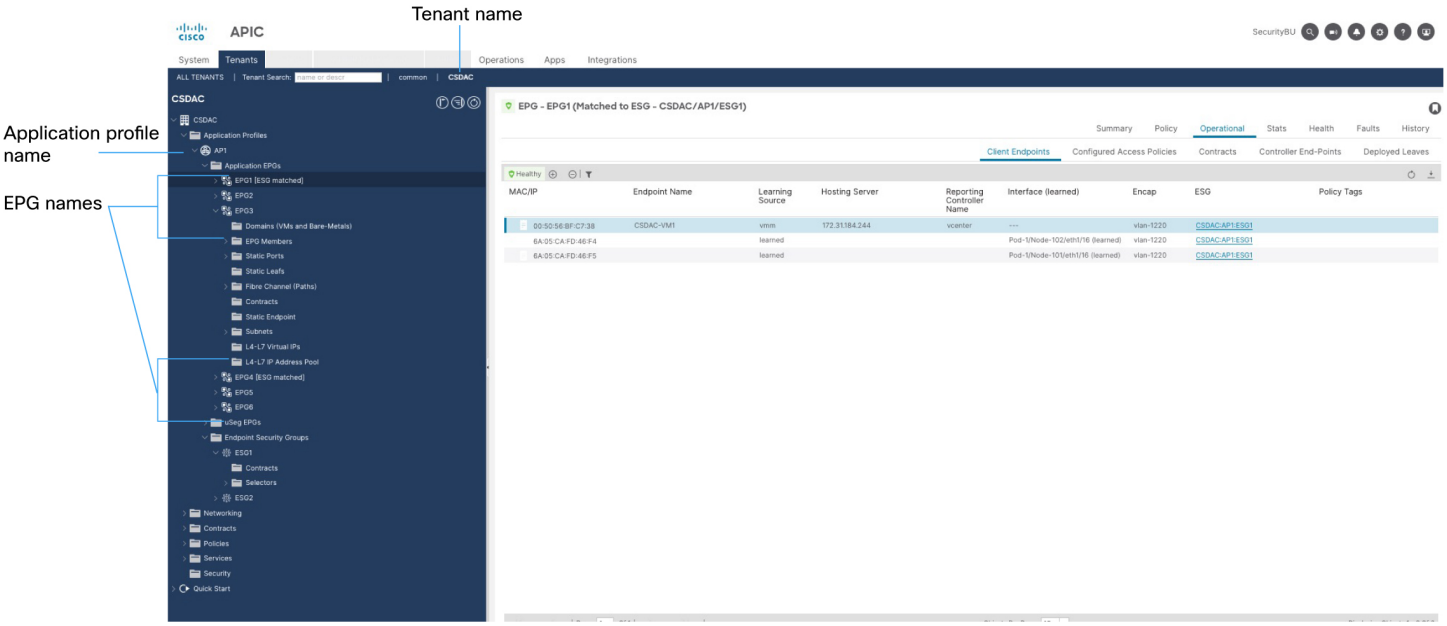
The following sample configuration shows how network object groups are named in ASA based on names in APIC and the APIC connector (not shown).

Network object group names are a concatenation of (in order):

- Cisco ACI Endpoint Update App **Site Prefix** value

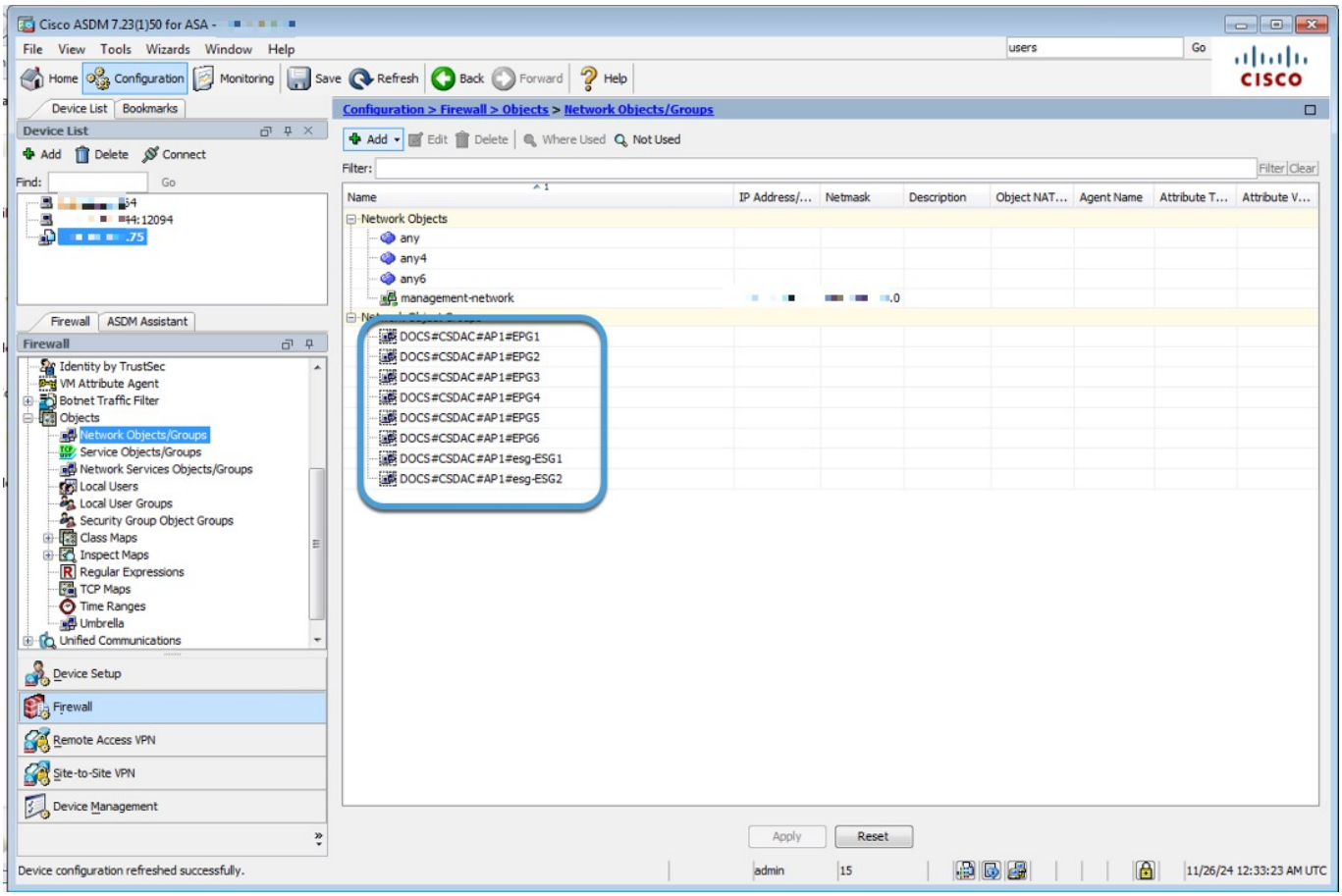
  Cisco APIC tenant name); in this example, `CSDAC`.

- Cisco APIC application profile name (in this example, `AP1`)
- Cisco APIC EPG name (in this example, `EPG1` through `EPG4`)



Assuming the connector's Site Prefix is DOCS and the Cisco APIC tenant name the `CSDAC` user has rights to is CSDAC, network object groups on ASA are named as follows (in ASDM, **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**):

About the Cisco APIC Integration with ASA



Additional information about Cisco APIC

- Basic User Tenant Configuration
- EPGs
- ESGs

Additional information about the Cisco Secure Dynamic Attributes Connector

Cisco%20Secure%20Dynamic%20Attributes%20Connector%20Configuration%20Guide.

What to do next

See Get Required Information for the Cisco APIC Integration with ASA.

How to Use Network Object Groups from Cisco APIC in ASA Access Rules

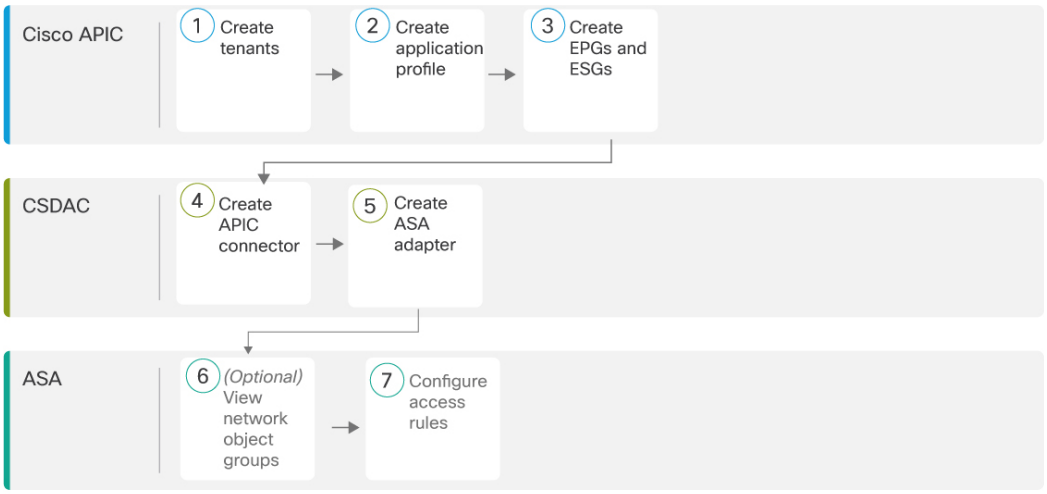


Table 1: Configure ASA access control policies using network object groups

1	Cisco APIC	A tenant allows a Cisco APIC administrator to set up domain-based access control. See Basic User Tenant Configuration
2	Cisco APIC	An application profile is a container for other objects, such as an endpoint group (EPG). See Basic User Tenant Configuration
3	Cisco APIC	An EPG is a container for network objects that serves as the way that devices connect to the network. An ESG is a logical entity that contains a collection of physical or virtual network endpoints. See EPGs and ESGs
4	Cisco Secure Dynamic Attributes Connector	The Cisco APIC connector retrieves network object groups from Cisco APIC periodically. As the objects or the IP addresses in them change, ASA is updated dynamically without the need to redeploy access rules. See Create a Cisco APIC Connector
5	Cisco Secure Dynamic Attributes Connector	The ASA adapter is responsible for updating objects on ASA. See Create an ASA Adapter

6	ASA	(Optional.) View the network object groups fetched from Cisco APIC. (Optional). See View Network Object Groups in ASDM
7	ASA	To use network object groups in access rules, you must add them as source criteria to those rules. See Add Network Object Groups to Access Rules