



# FortiOS - Cisco ACI Administration Guide

Version 6.4

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



March 06, 2024

FortiOS 6.4 Cisco ACI Administration Guide

01-640-656130-20240306

# TABLE OF CONTENTS

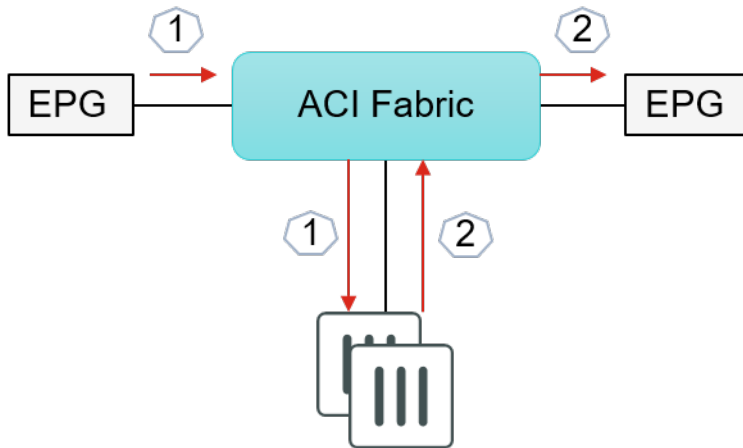
<b>HA on Cisco ACI using FGCP over FGSP</b> .....	<b>4</b>
FGCP over FGSP with ACI integration with example .....	6
Configuring the Cisco APIC management console .....	7
Configuring FortiOS .....	12
<b>SDN Connector integration with Cisco ACI</b> .....	<b>17</b>
Off-the-box connector VM .....	17
Configuring the Cisco ACI connector in FortiOS .....	17
Configuring VDOM and SDN connector example .....	17
FortiGate built-in connector .....	55
Configuring Cisco pxGrid SDN connector .....	58
Multiple clusters on Cisco ACI connectors .....	62
<b>Change log</b> .....	<b>67</b>

# HA on Cisco ACI using FGCP over FGSP

In Cisco ACI, you can deploy the FortiGate Clustering Protocol (FGCP) over the FortiGate Session Life Support Protocol (FGSP) to achieve high availability (HA). This deployment uses the following Cisco ACI components:

Component	Description
Endpoint group (EPG)	Container for collections of applications that is independent of addressing, VLAN, and other network components.
Contract	Defines communication between EPGs.
Service graph	Provides the capability to insert L4-L7 devices (in this case, the FortiGate) into Cisco ACI. Includes the policy-based redirect (PBR) feature, where the Cisco ACI fabric redirects traffic between security zones to the firewall (the FortiGate in this case) for inspection without requiring the firewall to be configured as the servers' default gateways. This provides increased stability by minimizing network changes.
Leaf and spine switches	Switches in Cisco ACI spine and leaf architecture, where there are two layers of switches: spine and leaf. The spine layer is the backbone of the network and interconnects all leaf switches. Leaf switches are access switches that connect to devices such as servers. See <a href="#">Cisco Data Center Spine-and-Leaf Architecture: Design Overview White Paper</a> .
Pod	Set of interconnected Cisco ACI leaf and spine switches that a specific Cisco Application Policy Infrastructure Controller (APIC) cluster is managing. Pods that the same APIC cluster is managing are considered part of the same Cisco ACI Fabric.
Inter-pod network (IPN)	Connects pods to allow for establishment of pod-to-pod communication (east-west traffic).
Tenant	Highest-level object in the ACI Fabric that contains EPGs and bridge domains (BDs).
Bridge domain	Domain that carries out forwarding and bridging processes.

In this deployment, traffic is redirected to the FortiGate for inspection. After inspection, FortiGate forwards the traffic to the Cisco ACI. The FortiGate is in one-arm mode in this scenario. This configuration supports asymmetric traffic flow, where the original and return traffic are inspected by different FortiGates.

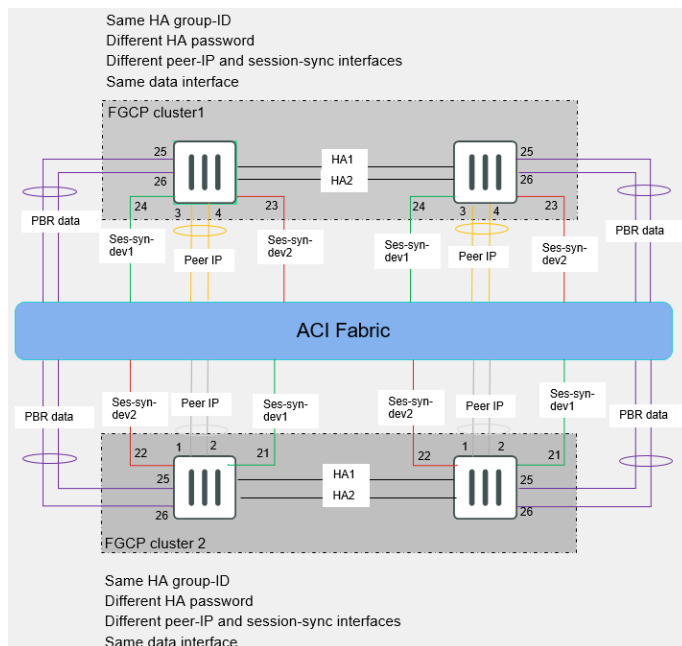


This solution uses Cisco ACI service chaining with PBR and the Anycast feature. The topology for this deployment is as follows:

- Two FGCP clusters:
  - Each cluster in a different pod
  - Each cluster has two FortiGate
- FGSP across all pods

This deployment requires the following configurations:

- Due to the Cisco ACI requirement to have an Anycast IP address and a MAC address, you must configure both FGCP clusters with the same HA group ID.
- PBR data interface must use the same ports on both clusters.
- One VLAN is created for traffic processing. It has the same IP and MAC addresses on both clusters.
- `peer-ip` and `session-sync-device` use different ports with different MAC addresses.

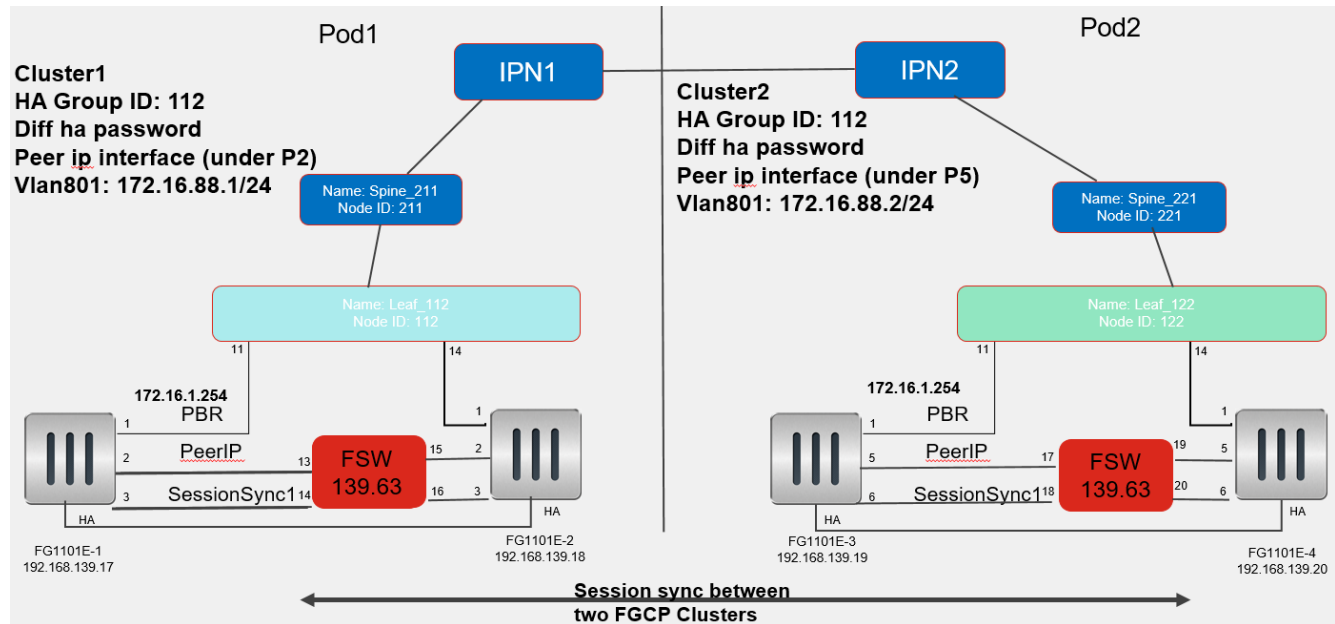


As no provisioning configuration is pushed from the APIC to the FortiGate, importing a device package to APIC is not required.

## FGCP over FGSP with ACI integration with example

In this example, the configuration is achieved using FortiGate 1101E running FortiOS 6.4.2 and Cisco ACI 5.2.

The following diagram shows the topology for this example configuration, which consists of two pods.

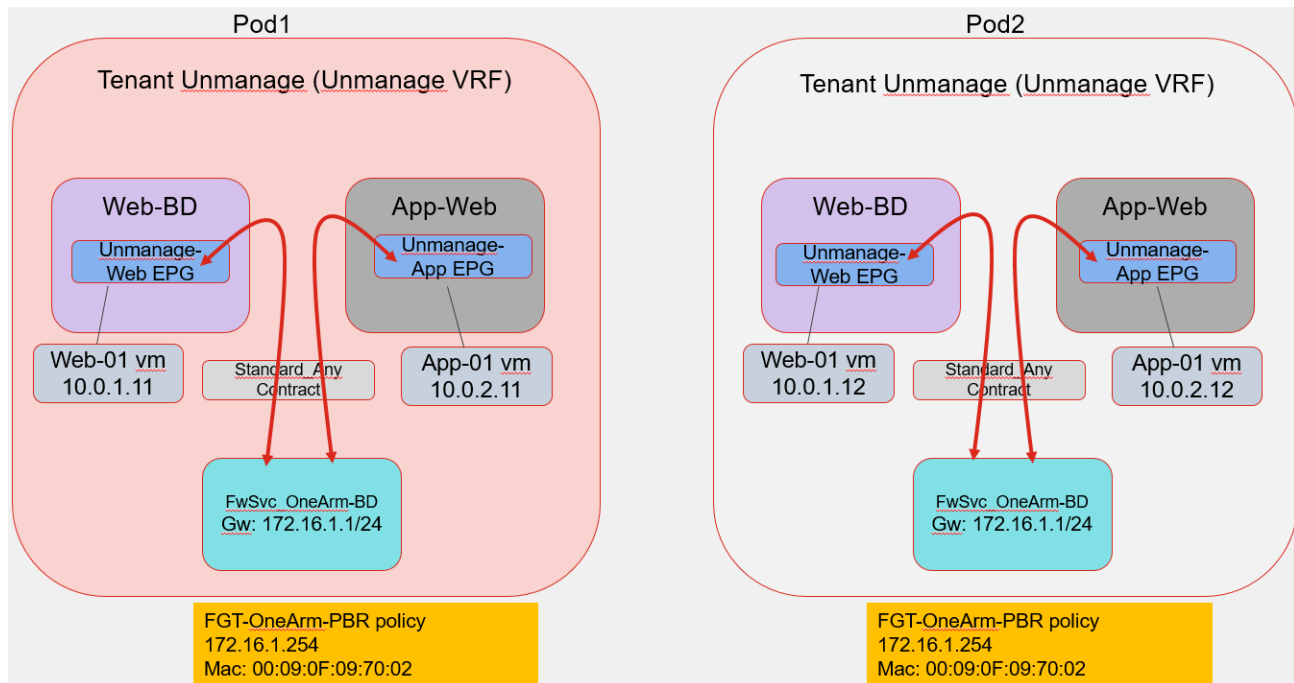


The configuration has the following settings:

- Each pod contains a FGCP cluster with two FortiGate 110Es.
- The pods communicate via their IPNs.
- The clusters share the same HA group ID, 112.
- The clusters share the same VLAN, VLAN801, with IP address 172.16.88.1/24.
- The clusters have different HA passwords.
- Peer IP interfaces are configured as follows. If you do not disable the port that the other cluster is using for its peer IP interface, the peer IP interface connected to the switch will detect the same VMAC over multiple interfaces, due to having the same HA group ID with the same VMAC with interfaces enabled:
  - For cluster1, the peer IP interface is under port2. Port5 is disabled on cluster1 FortiGates.
  - For cluster2, the peer IP interface is under port5. Port2 is disabled on cluster2 FortiGates.
- There is session synchronization between the two clusters. Session synchronization is configured as follows. If you do not disable the port that the other cluster is using for session synchronization, session synchronization does not work as it is unable to learn the peer FGCP VMAC, due to having the same HA group ID with the same VMAC with interfaces enabled.
  - Cluster1 uses port3 for session synchronization. Port6 is disabled on cluster1 FortiGates.
  - Cluster2 uses port6 for session synchronization. Port3 is disabled on cluster2 FortiGates.
- Both clusters have the state of the session and the session will not be dropped.

In a production environment, configuring multiple `session-sync-dev` interfaces for load balancing session sync packets is recommended.

The following diagram provides a more detailed view of what occurs at the leaf level. Each pod contains a Tenant (here named "Unmanage"), which contains three BDs: Web, App, and FwSvc\_OneArm-BD. The Web and App BDs each contain an EPG with a virtual machine. A contract defines communication between the Web and App EPGs. Traffic flow between the Web and APP EPGs uses the PBR policy to flow to the FortiGate for inspection, and to its destination after inspection.



The following steps assume that a tenant is already created.

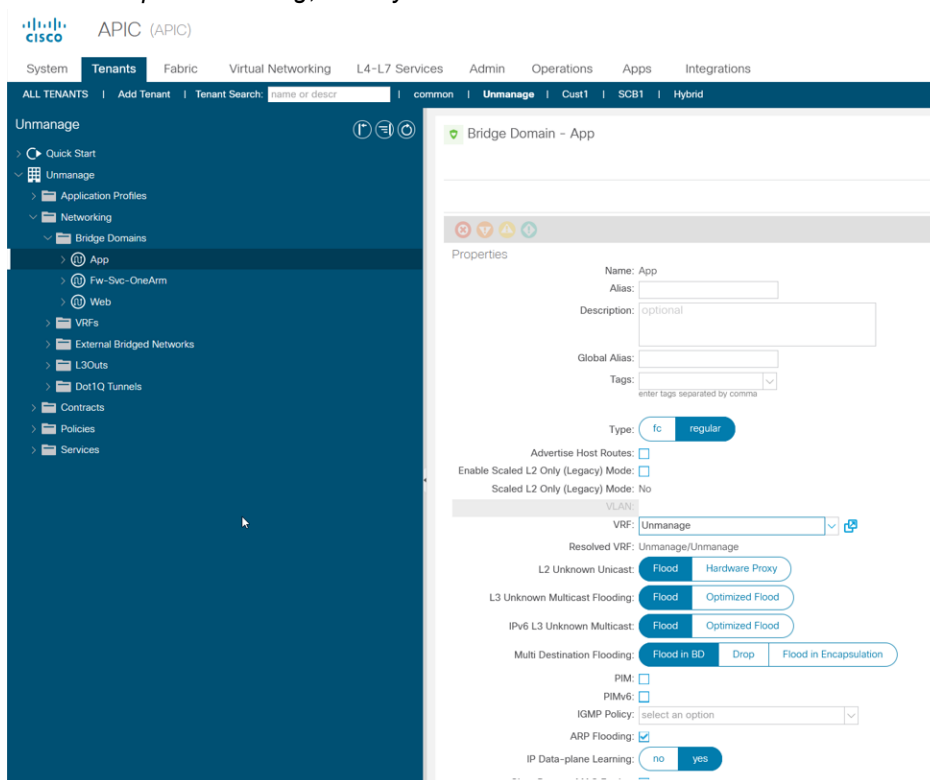
You must configure the deployment on the Cisco APIC management console, then configure the necessary options in FortiOS.

## Configuring the Cisco APIC management console

**To configure the deployment on the Cisco APIC management console:**

1. Log in to the Cisco APIC management console.
2. Configure the BDs:
  - a. On the *Tenants* tab, go to *Unmanage > Networking > Bridge Domains*.
  - b. Configure the App BD:
    - i. Click *Add Tenant*.
    - ii. In the *Name* field, enter *App*.

iii. For *IP Data-plane Learning*, select *yes*.



c. Configure the Web BD:

i. Click *Add Tenant*.

ii. In the *Name* field, enter *Web*.

iii. For *IP Data-plane Learning*, select *yes*.

d. Configure the Fw-Svc-OneArm BD:

i. Click *Add Tenant*.

ii. In the *Name* field, enter *Fw-Svc-OneArm BD*.

iii. For *IP Data-plane Learning*, select *no*.

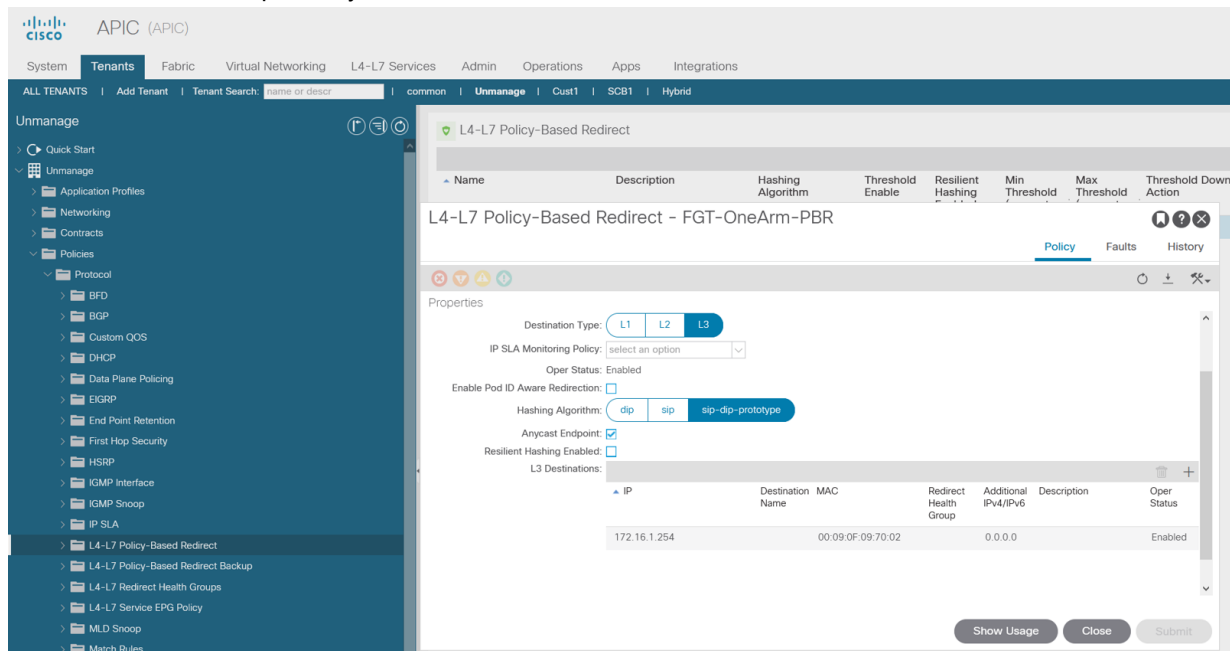
3. Go to *Policies*. Configure a PBR policy:

a. Enable *Anycast Endpoint*. This is required to allow the traffic to flow through either cluster.

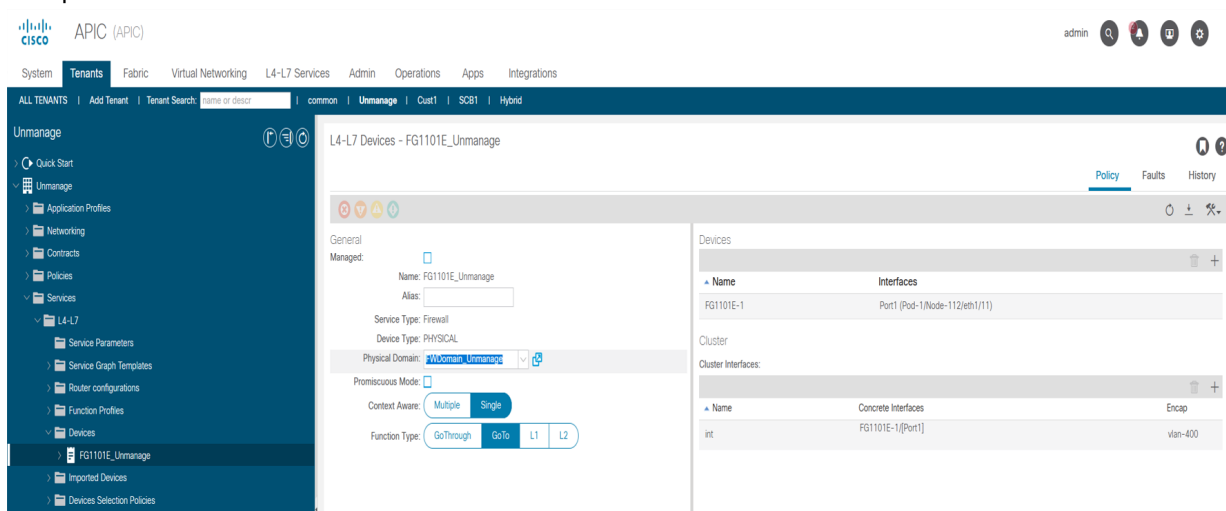
b. Under *L3 Destinations*, add the PBR IP and MAC addresses. In this case, the addresses are 172.16.1.254 and



00:09:0F:09:70:02, respectively.

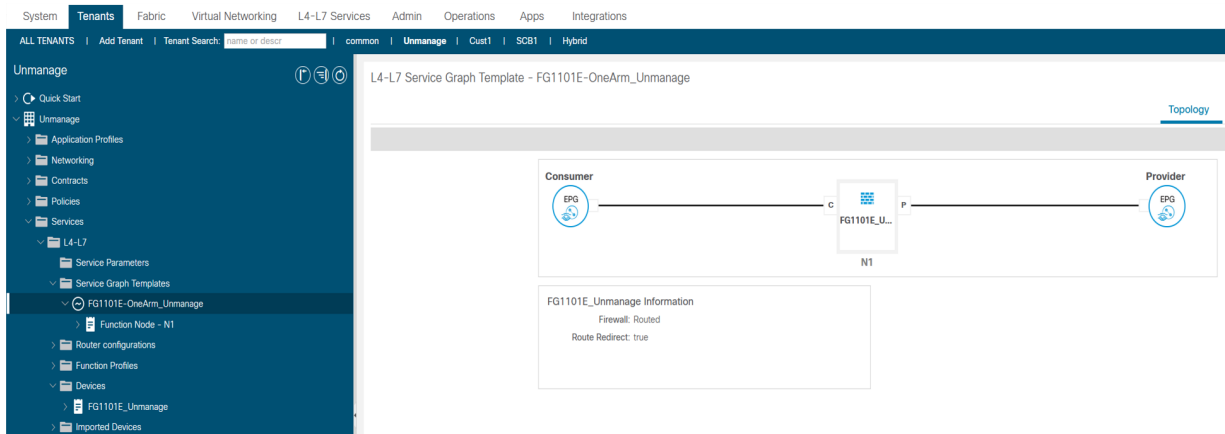


4. Configure an L4-L7 device:
  - a. Go to *Services > L4-L7 > Devices*.
  - b. Create a new device.
  - c. Ensure that *Managed* is unselected.
  - d. From the *Physical Domain* dropdown list, select *FWDomain\_Unmanage*.
  - e. Under *Devices*, add the FortiGate. In this example, the device name is FG1101E-1, and the interface is Port1.
  - f. Under *Cluster Interfaces*, add the FG1101E-1 port1 as a concrete interface and vlan-400 as the encapsulation.



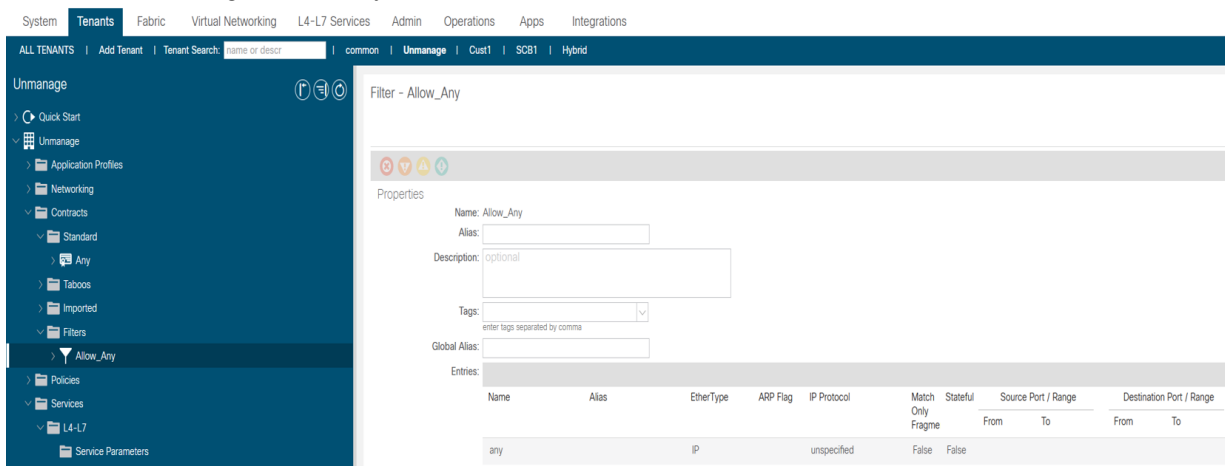
5. Configure the service graph template:
  - a. Go to *Services > L4-L7 > Service Graph Templates*.
  - b. Create a new service graph template that goes from the consumer (Web EPG) to the L4-L7 device that you create to the provider (App EPG).
  - c. For *Firewall*, select *Routed*.

- d. For *Route Redirect*, select *true*.



6. Create a filter:

- a. Go to *Contracts > Filters*.
- b. Create a new contract.
- c. In the *Name* field, enter *Allow\_Any*.
- d. Under *Entries*, configure one entry that allows all traffic.



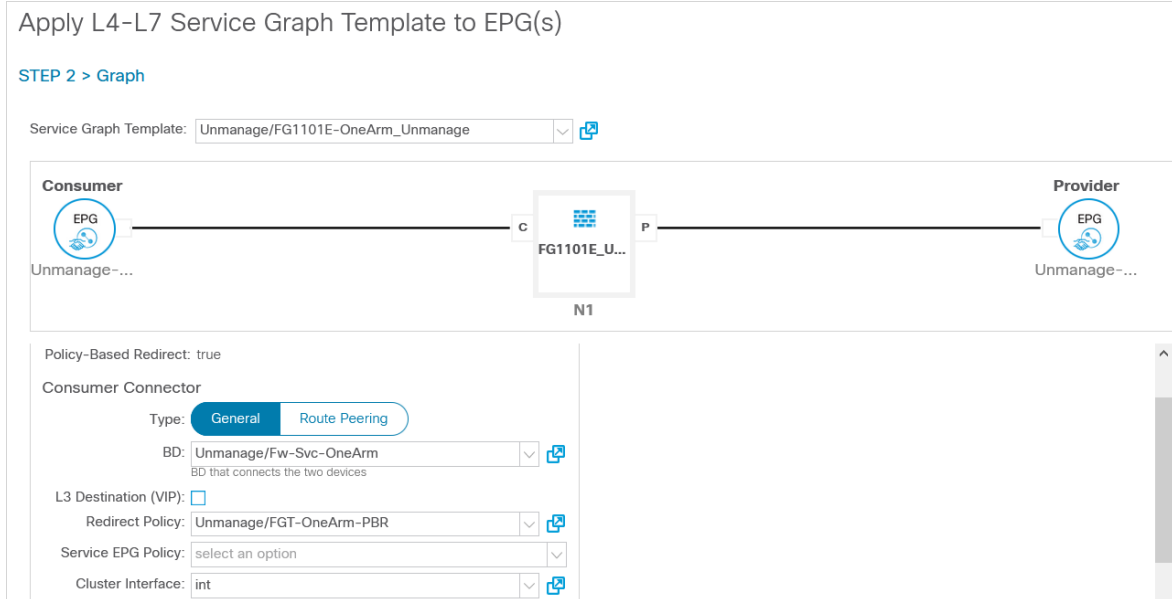
7. Configure the contract:

- a. Go to *Contracts > Standard*.
- b. Create a new contract.
- c. Under *Subjects*, configure the *Allow\_Any* filter. This contract is now applied between the Web and App EPGs. At this point, when the firewall integration is not configured, the Web and App EPGs can communicate freely without any inspection.

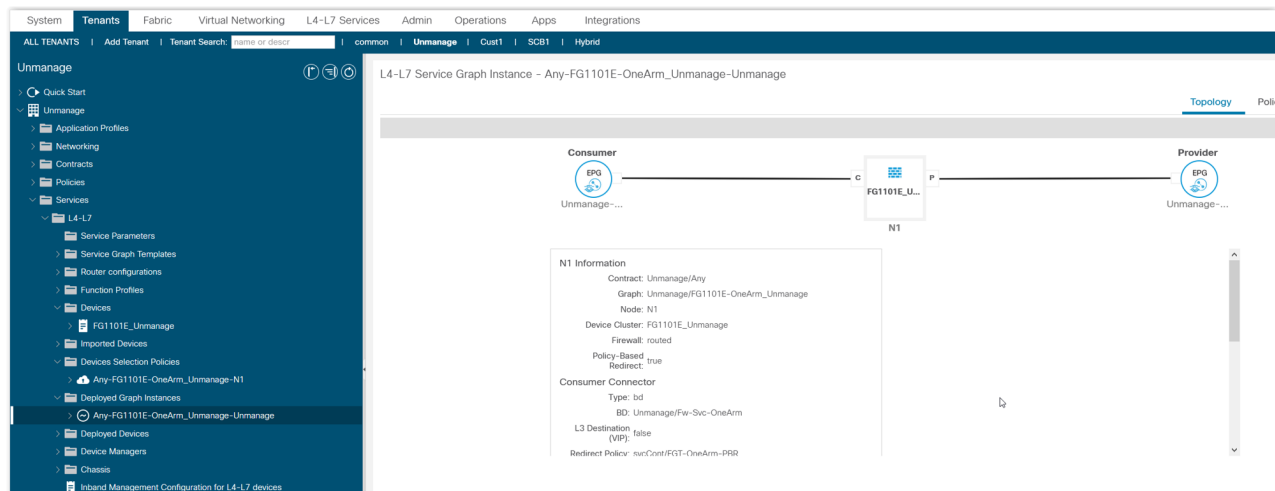
8. Apply the service graph template:

- a. Under *Services > L4-L7 > Service Graph Templates*, right-click the service graph template that you created, and select *Apply L4-L7 Service Graph Template*.
- b. From the *Consumer EPG / External Network* dropdown list, select the Web EPG.
- c. From the *Provider EPG / Internal Network* dropdown list, select the App EPG.
- d. For *Contract Type*, select *Select Existing Contract Subject*.
- e. From the *Existing Contracts with Subjects* dropdown list, select *Allow\_Any*.
- f. From the *Service Graph Template* dropdown list, select *FG1101E-OneArm\_Unmanage*.

- g. Under *Consumer Connector*, configure the following:
  - i. From the *BD* dropdown list, select *Fw-Svc-OneArm*.
  - ii. From the *Redirect Policy* dropdown list, select *FGT-One-Arm-PBR*.
  - iii. Leave the *Service EPG Policy* field empty.
  - iv. From the *Cluster Interface* dropdown list, select *int*.



- h. Under *Provider Connector*, configure the following:
  - i. For *Type*, select *General*.
  - ii. Configure other fields with the same values as for the consumer connector.
9. Configure a device selection policy:
  - a. Go to *Services > L4-L7 > Devices Selection Policies*.
  - b. Create a new policy.
  - c. For the contract, select *Any*.
  - d. For the graph, select *FG1101-OneArm\_Unmanage*.
  - e. From the *Devices* dropdown list, select *FG1101E\_Unmanage*.
10. Go to *Services > L4-L7 > Deployed Graph Instances*. Confirm that you can see that the configured service graph has been deployed as configured.



## Configuring FortiOS

### To configure the deployment in FortiOS:

1. Create a PBR virtual domain (VDM). You must make all following configurations in the PBR VDM.
2. Configure a VLAN interface under port 1 with VLAN ID 400:
  - a. Go to *Network > Interfaces*.
  - b. Click *Create New*.
  - c. In the *Name* field, enter *vlan400*.
  - d. For *Type*, select *VLAN*.
  - e. For *Interface*, select *port1*.
  - f. In the *VLAN ID* field, enter 400.
  - g. In the *VRF ID* field, enter 0.
  - h. From the *Role* dropdown list, select *LAN*.

- i. In the *IP/Netmask* field, enter 172.16.254/255.255.255.0. Save the interface.

3. Go to *Policy & Objects > Firewall Policy*. Configure policies as desired.
4. Configure a static route to the APIC FW\_Svc\_OneArm BD GW IP address:
  - a. Go to *Network > Static Routes*.
  - b. Click *Create New*.
  - c. Set *Destination* to *Subnet*, and leave the IP address and subnet mask as 0.0.0.0/0.0.0.0.
  - d. In the *Gateway Address* field, enter the APIC FW\_Svc\_OneArm BD GW IP address, which is 172.16.1.1.
  - e. From the *Interface* dropdown list, select vlan400.
  - f. Save the configuration.

Destination	Gateway IP	Interface	Status
0.0.0.0/0	172.16.1.1	vlan400	Enabled

5. Go to *Log & Report > Forward Traffic*. Confirm that you can view the Web and Application EPG traffic, indicating that it is redirected to the FortiGate for inspection.

Date/Time	Source	Device	Destination	Application Name	Result	Polic
32 minutes ago	10.0.1.11	00:50:56:b4:01:c8	10.0.2.11		3.19 kB / 3.19 kB	Allow_All (1)
32 minutes ago	10.0.2.11	00:50:56:b4:37:ab	10.0.1.11		168 B / 168 B	Allow_All (1)
32 minutes ago	10.0.1.11	00:50:56:b4:01:c8	10.0.2.11		168 B / 168 B	Allow_All (1)
33 minutes ago	10.0.2.11	00:50:56:b4:37:ab	10.0.1.11		2.44 kB / 2.44 kB	Allow_All (1)

6. Run the following commands in the CLI to configure FGCP and FGSP for cluster1:

```
config system ha
  set group-id 112
  set group-name "fortinet112"
  set mode a-p
  set pass ENC 6v7bvUAMnjUK8GLToPP4ctq9GdqRH37cZ01WfMbJzBTXg53bc8KF1C0QFhk9AEzen695Q
  set hbdev "ha" 512
  set session-pickup enable
  set session-pickup-connectionless enable
  set session-pickup-expectation enable
  set ha-mgmt-status enable
  config ha-mgmt-status enable
    edit 1
      set interface "mgmt"
```

```

        set gateway 192.168.139.254
    next
end
set override disable
set ha-direct enable
end
config system cluster-sync
    edit 5
        set peerip 172.16.88.2
        set syncvd "PBR"
    next
end
config system standalone-cluster
    set standalone-group-id 112
    set session-sync-dev "port3"
end

```



By default, FortiOS sets layer2-connection to unavailable. If layer2-connection is set to available, the configuration may have issues.

---

**7. Run the following commands in the CLI to configure FGCP and FGSP for cluster2:**

```

config system ha
    set group-id 112
    set group-name "fortinet112112"
    set mode a-p
    set pass ENC bhU6+uYFf7IpqOirYnFWOMhGxbpJkXY8bdHWfg9o6x2Wg+IFId6ZEJUGqe2Wlots+g==
    set hbdev "ha" 512
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-expectation enable
    set ha-mgmt-status enable
    config ha-mgmt-status enable
        edit 1
            set interface "mgmt"
            set gateway 192.168.139.254
        next
    end
    set override disable
    set ha-direct enable
end
config system cluster-sync
    edit 5
        set peerip 172.16.88.2
        set syncvd "PBR"
    next
end
config system standalone-cluster
    set standalone-group-id 112
    set group-member-id 1
    set session-sync-dev "port6"
end

```



By default, FortiOS sets `layer2-connection` to `unavailable`. If `layer2-connection` is set to `available`, the configuration may have issues.

8. To debug cluster1, you can run the following commands. The screenshot shows the expected output of each command:

a. `diagnose system ha status`

```
HA information
Statistics
    traffic.local = s:0 p:1198673 b:436792155
    traffic.total = s:0 p:1198676 b:436790922
    activity.ha_id_changes = 3
    activity.fdb = c:0 q:0

Model=1000, Mode=2 Group=112 Debug=0
nvcluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FG10E1TB20900659: Primary, serialno_prio=0, usr_priority=128, hostname=FG1101E-1
FG10E1TB20900658: Secondary, serialno_prio=1, usr_priority=128, hostname=FG1101E-2

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.1, primary_id=0:
FG10E1TB20900659: Primary, ha_prio/o_ha_prio=0/0
FG10E1TB20900658: Secondary, ha_prio/o_ha_prio=1/1
```

b. `diagnose system ha standalone-peers`

```
Group=112, ID=0
Detected-peers=1
Kernel standalone-peers: num=1.
peer0: vfid=0, peerip:port = 172.16.88.2:708, standalone_id=1
    session-type: send=0, recv=595
    packet-type: send=0, recv=0
Kernel standalone dev_base:
    standalone_id=0:
        phyindex=0: mac=e0:23:ff:01:86:f5, linkfail=1
        phyindex=1: mac=e0:23:ff:01:86:f4, linkfail=1
        phyindex=2: mac=e0:23:ff:01:86:d5, linkfail=1
        phyindex=3: mac=e0:23:ff:01:86:d6, linkfail=1
        phyindex=4: mac=e0:23:ff:01:86:d7, linkfail=1
```

c. `diagnose system ha session-sync-dev`

```
HA sessync ports: 1
port3 connected: HA connected, Standalone connected
HB pkts: rx=4490, tx=2284
SES pkts: rx=762, tx=235
```

9. To debug cluster2, you can run the following commands. The screenshot shows the expected output of each command:

## a. diagnose system ha status

```

HA information
Statistics
    traffic.local = s:0 p:101310 b:39959406
    traffic.total = s:0 p:104820 b:40312857
    activity.ha_id_changes = 2
    activity.fdb = c:0 q:0

Model=1000, Mode=2 Group=112 Debug=0
nvcluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FG10E1TB20900643: Primary, serialno_prio=0, usr_priority=128, hostname=FG1101E-3
FG10E1TB20900230: Secondary, serialno_prio=1, usr_priority=128, hostname=FG1101E-4

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.1, primary_id=0:
FG10E1TB20900643: Primary, ha_prio/o_ha_prio=0/0
FG10E1TB20900230: Secondary, ha_prio/o_ha_prio=1/1

```

## b. diagnose system ha standalone-peers

```

Group=112, ID=1
Detected-peers=1
Kernel standalone-peers: num=1.
peer0: vfid=0, peerip:port = 172.16.88.1:708, standalone_id=0
    session-type: send=0, recv=0
    packet-type: send=0, recv=0
Kernel standalone dev_base:
    standalone_id=0:
        phyindex=0: mac=00:09:0f:09:70:00, linkfail=1
        phyindex=1: mac=e0:23:ff:01:86:f4, linkfail=1
        phyindex=2: mac=00:09:0f:09:70:02, linkfail=1
        phyindex=3: mac=00:09:0f:09:70:03, linkfail=1
        phyindex=4: mac=00:09:0f:09:70:04, linkfail=1
        phyindex=5: mac=00:09:0f:09:70:05, linkfail=1

```

## c. diagnose system ha session-sync-dev

```

HA sessync ports: 1
port6 connected: HA connected, Standalone connected
HB pkts: rx=4905, tx=2380
SES pkts: rx=145, tx=861

```



# SDN Connector integration with Cisco ACI



Fortinet Device Package for Cisco ACI is being deprecated. Use an SDN connector that this document describes as a replacement.

---

## Off-the-box connector VM

You can use Cisco ACI (Application Centric Infrastructure) SDN connectors in dynamic firewall addresses.

The Fortinet SDN Connector for Cisco ACI is a standalone connector that connects to SDN controllers within Cisco ACI. You must configure a connection to the Fortinet SDN connector in FortiOS to query the dynamic addresses.

## Configuring the Cisco ACI connector in FortiOS

See the [FortiOS Administration Guide](#).

## Configuring VDOM and SDN connector - example

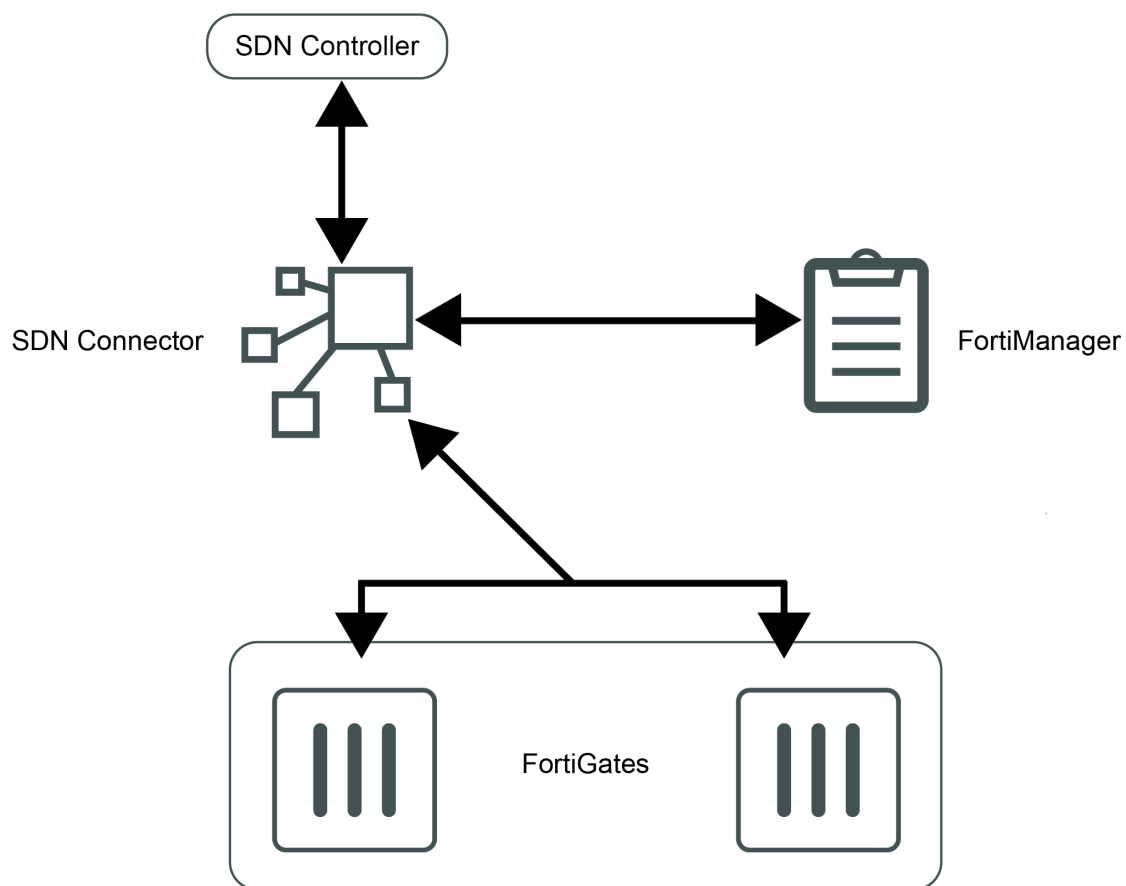
SDN Connector is the Fortinet response to integrate various SDN solutions with FortiGate as well as FortiManager products. The SDN Connector serves as a gateway bridging SDN controllers and Fortinet devices including FortiGate and FortiManager. The SDN Connector registers itself to the Cisco ACI SDN controller, polls interested objects, and translates them into address objects. The translated address objects and associated endpoints are populated to the FortiGate/FortiManager that are interested in these objects.

The following provides an example of configuring VDOM and SDN Connector. This example uses SDN Connector 1.1.3.

### Overview

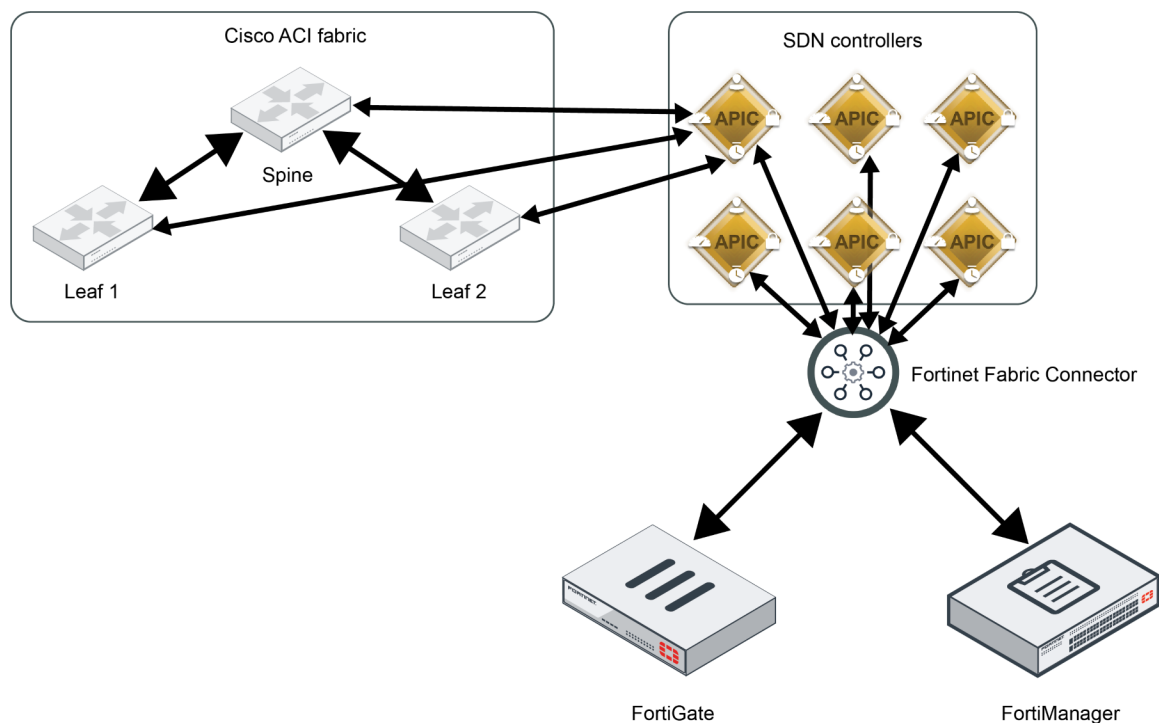
### Components

The following diagram illustrates the relationship between the components of the SDN Connector:



## Topology

The following diagram illustrates the topology when using SDN Connector with FortiManager:



## Licensing

SDN Connector is available free of charge for Fortinet customers. You must ensure that you register your FortiGate/FortiManager with FortiCare on [Fortinet Customer Service & Support](#).

## Hardware requirements

If you plan to instantiate a large number of virtual machines (VMs) in your SDN Connector environment, ensure that you size the host VM or server appropriately. The following recommendations represent the minimum sizing numbers:

- Memory: 4 GB
- CPU: 2 vCPU
- Disk: 20-50 GB
- vNICs: 1

## Terminology

The following defines some terms used in this guide:

ACI	Cisco Application Centric Infrastructure
APIC	Cisco Application Policy Infrastructure Controller
BD	Bridge domain
EPG	Endpoint group
VDOM	Virtual domain
SDN	Software-defined network

## Supported new features

SDN Connector 1.1 supports the Nuage and Cisco ACI platforms. This guide is written for the Cisco ACI platform.

## Supported Fortinet products

All physical and virtual FortiGate products that support the Fortinet Security Fabric are compatible with SDN Connector. FortiManager-VM has also been qualified.

## Firmware versions

SDN Connector 1.1 is compatible with the following FortiOS versions:

- 6.2.0 and later versions
- 6.0.5

## Prerequisites

The following prerequisites must be met before deploying SDN Connector with Cisco ACI Connector:

- [Cisco-side prerequisites on page 20](#)
- [FortiGate-side prerequisites on page 20](#)
- [FortiManager-side prerequisites on page 21](#)
- [SDN Connector prerequisites on page 21](#)
- [Cisco ACI deployment on page 28](#)

### Cisco-side prerequisites

Before you can successfully deploy SDN Connector, a number of prerequisites must be satisfied within the Cisco environment. A Cisco ACI 3.0 or later environment must be in place. Within Cisco, the following configurations must be completed before SDN Connector can pull objects:

- Creation of Access Policies configuration under the *Fabric* menu
- Creation of any needed tenant(s)
- Creation of network(s) including BD
- Creation of application profile(s)
- Creation of EPG(s)
- Creation of contract(s)
- Create BG/OSPF L3Out (only if BGP/OSPF is required)

For details, consult the [Cisco APIC deployment guide](#).

### FortiGate-side prerequisites

Before you can successfully deploy SDN Connector, a number of prerequisites must be satisfied on the FortiGate:

1. Configure the administrator username and password.
2. Enable HTTP/HTTPS on the management port.
3. Configure the management port's IP address.

4. Enable VDOM-Admin globally.
5. Configure port-group if needed.

### FortiManager-side prerequisites

Before you can successfully deploy SDN Connector, a number of prerequisites must be satisfied on FortiManager:

1. Configure the administrator username and password.
2. Enable HTTP/HTTPS on the management port.
3. Configure the management port's IP address.
4. Register the FortiGate with FortiManager.

### SDN Connector prerequisites

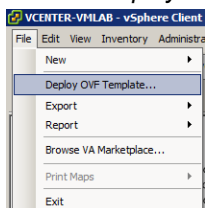
Before you can successfully deploy SDN Connector, you must complete a number of tasks on the SDN Connector:

### Installing the SDN Connector

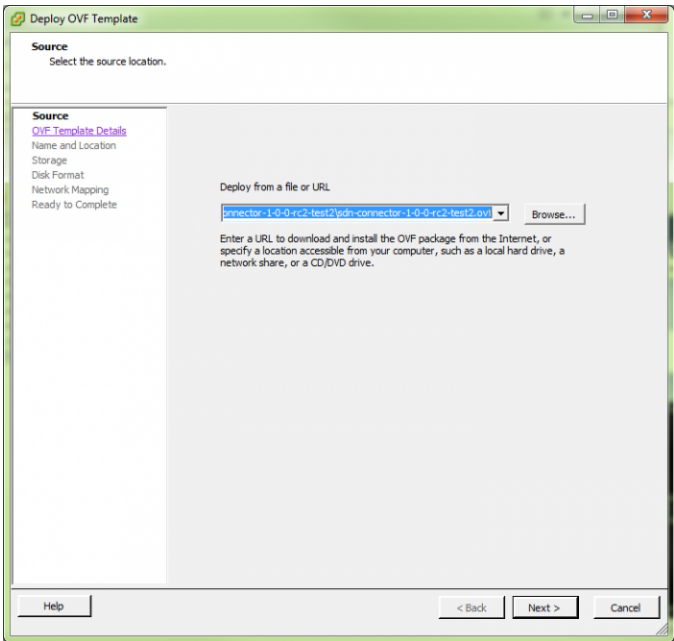
1. SDN Connector supports VMware vSphere, KVM, and Microsoft Hyper-V as deployment environments. Download the connector package:
  - a. On the [Customer Service & Support site](#), go to *Download > Firmware Images*.
  - b. From the *Select Product* dropdown list, select *FortiSDNConnector*.
  - c. On the *Download* tab, go to *v1.00 > v1.1.3*.
  - d. Download the appropriate file based on your hypervisor platform:

Hypervisor	File
KVM	sdn-connector-1.1.3.img
Hyper-V	sdn-connector-1.1.3.vhd
VMware vSphere	sdn-connector-1.1.3.zip

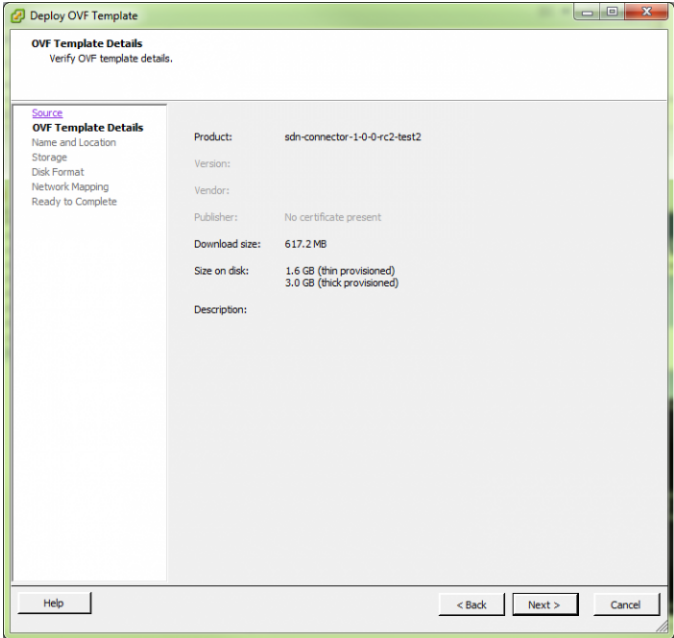
2. This example shows the installation process for vSphere client. Download sdn-connector.ovf. In vSphere Client, go to *File > Deploy OVF Template*.



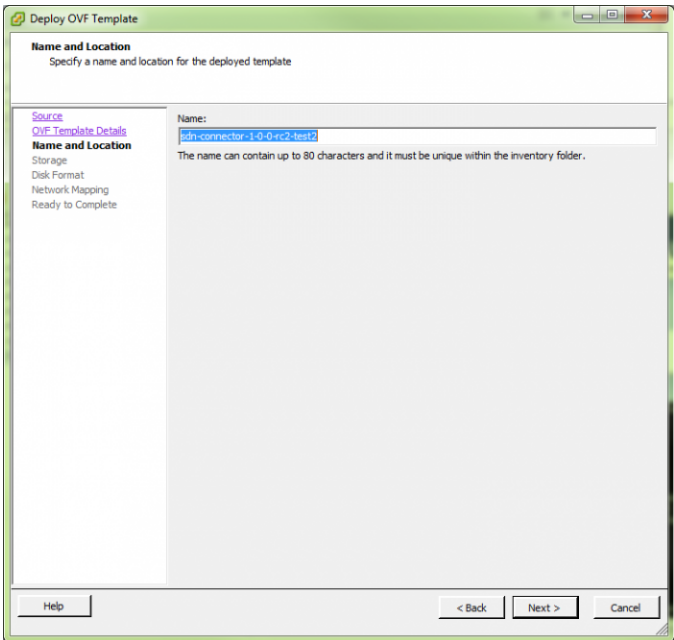
3. In the *Deploy OVF Template* dialog, enter the SDN Connector image file path in the *Deploy from a file or URL* field. Click *Next*.



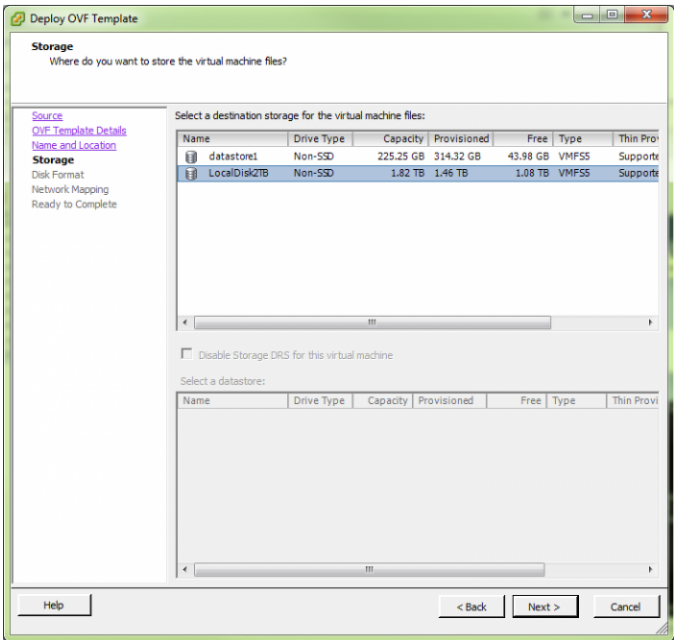
4. The dialog displays the SDN Connector version, download size, and size on disk. Click *Next*.



5. Enter the VM name, select the location, then click *Next*.



6. Choose the destination storage for the VM files, then click *Next*.



7. The dialog displays the datastore name and amount of available space. Select *Thin Provision*, then click *Next*.

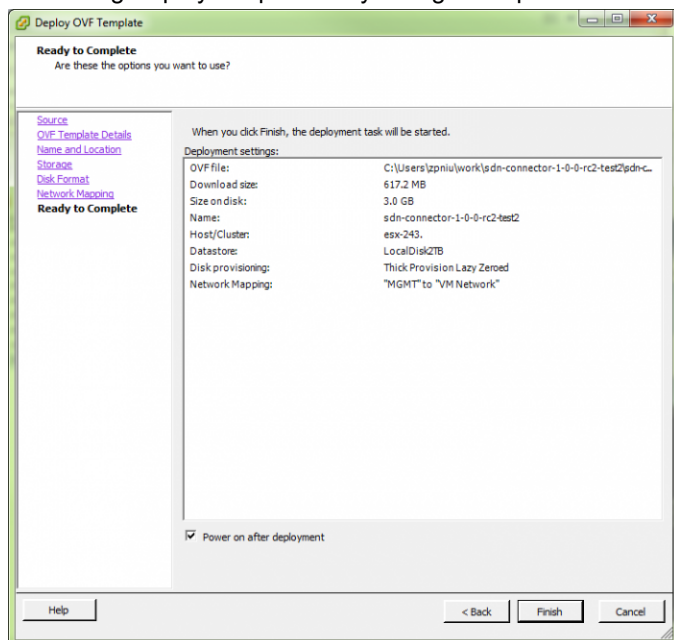
The screenshot shows the 'Deploy OVF Template' dialog box, specifically the 'Disk Format' step. The title bar says 'Deploy OVF Template'. The main heading is 'Disk Format' with the subtitle 'In which format do you want to store the virtual disks?'. On the left, there is a sidebar with links: 'Source', 'OVF Template Details', 'Name and Location', 'Storage', 'Disk Format' (selected), 'Network Mapping', and 'Ready to Complete'. The main area shows 'Datastore:' as 'LocalDisk2TB' and 'Available space (GB):' as '1104.6'. There are three radio button options: 'Thick Provision Lazy Zeroed' (selected), 'Thick Provision Eager Zeroed', and 'Thin Provision'. At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

8. Networks used in this OVF template should map to networks in your inventory. Choose the destination network for network mapping, then click *Next*.

The screenshot shows the 'Deploy OVF Template' dialog box, specifically the 'Network Mapping' step. The title bar says 'Deploy OVF Template'. The main heading is 'Network Mapping' with the subtitle 'What networks should the deployed template use?'. On the left, there is a sidebar with links: 'Source', 'OVF Template Details', 'Name and Location', 'Storage', 'Disk Format', 'Network Mapping' (selected), and 'Ready to Complete'. The main area has the instruction 'Map the networks used in this OVF template to networks in your inventory'. Below this is a table with two columns: 'Source Networks' and 'Destination Networks'. The first row shows 'MGMT' in the 'Source Networks' column and 'VM Network' in the 'Destination Networks' column. Below the table is a 'Description:' label and a text area containing 'The MGMT network:'. At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

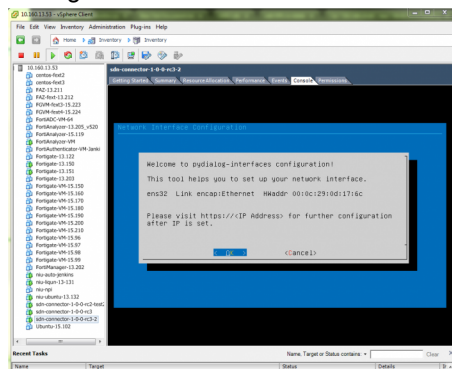


9. The dialog displays all previously configured options. To edit an option, click *Back*. If ready to deploy, click *Finish*.

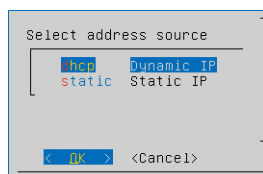


## Initializing the SDN Connector

1. After deploying the OVF template, turn on the VM and go to the *Console* tab. Once the SDN Connector boots up, the system displays the following GUI dialog for configuration. Press *Enter* to proceed to the Network Interface Configuration wizard.



The Network Interface Configuration wizard provides DHCP and static IP configuration options.



When the VM receives the IP address from the DHCP server, the system shows this success dialog. The dialog shows the SDN Connector IP address and gateway information.

```

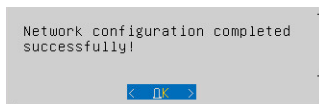
Network configuration completed successfully!

Internet Systems Consortium DHCP Client 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

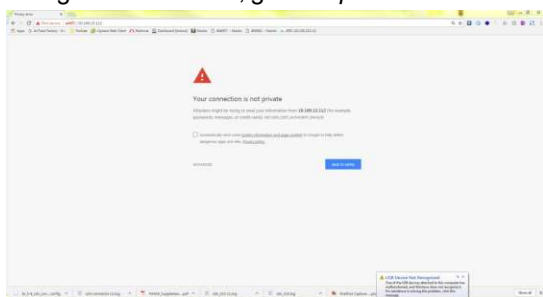
Listening on LPF/ens32/00:0c:29:8e:aa:d7
Sending on   LPF/ens32/00:0c:29:8e:aa:d7
Sending on   Socket/fallback
DHCPDISCOVER on ens32 to 255.255.255.255 port 67 interval 3
(xid=0x30ea567b)
DHCPRREQUEST of 10.160.13.112 on ens32 to 255.255.255.255 port 67
(xid=0x7b56ea30)
DHCPOFFER of 10.160.13.112 from 10.160.13.1
DHCPACK of 10.160.13.112 from 10.160.13.1
bound to 10.160.13.112 -- renewal in 290399 seconds.

```

When the VM is configured with a static IP address, the system shows this success dialog.



2. To change the network configuration, click **OK** and return to the wizard to restart the setup flow.
3. Using a web browser, go to <https://<SDN connector IP address>>.



4. Log into the system with the default username and password, which are `admin@sdn-connector.local` and `fortinet123`, respectively. When you first log in, the GUI prompts you to change the password.

Change Web GUI Password

Old Password

New Password

Repeat

Confirm New Password

Repeat

OK

Cancel

## Configuring the SDN Connector

The SDN Connector GUI has several web controls. It is a single-page web application.

To restart the service, click *Restart Service*. The system displays a dialog asking you to restart the connector service.



To change the password, click *Change Password*.

Change Web GUI Password

Old Password

New Password

Confirm New Password

OK Cancel

To change the configuration click *Configuration*.

Fortinet Fabric Connector

Configuration

Running Status

Cache Content

Download Log

SDN Controller Type

aci

APIC Host/IP

10.105.152.11, 10.105.152.12, 10.105.152.13

APIC Username

admin

APIC Password

\*\*\*\*\*

\*\*\*\*\*

OK Cancel

Fabric Connector IP

localhost

Fabric Connector Username

admin

Change Fabric Connector Password

\*\*\*\*\*

\*\*\*\*\*

Log Level

info

Upgrade

The *Configuration* page consists of the following fields:

Option	Description
APIC Host/IP	You can enter multiple APIC IP addresses and/or FQDNs. Ensure that you separate each entry with a comma.
APIC Username	Enter the Cisco ACI username as obtained from the ACI administrator.
APIC Password	Enter the Cisco ACI password as obtained from the ACI administrator.
Fabric Connector Username	Enter the FortiGate/FortiManager username used to log into the Fortinet SDN connector. The default username is admin.
Change Fabric Connector Password	Enter the FortiGate/FortiManager password used to log into the Fortinet SDN connector. The default password is fortinet123.

To upgrade the service, go to the SDN Connector homepage, then click *UpgradeService* on the banner. A dialog shows the upgrade progress. Once the upgrade is finished, the dialog prompts *“Upgraded Successfully! Going to refresh in 10s”* and the GUI refreshes automatically. This allows patch upgrade for SDN Connector.

Upgrade SDN Connector Software

File Path

Select File(tar.gz or whl)

Upload Cancel

The following displays sample output objects pulled from Cisco ACI:



named "vrf1".

The screenshot shows the 'Create Tenant' form in the Cisco APIC interface. The 'Name' field is highlighted with a red box and contains 'Tenant1'. The 'VRF Name' field at the bottom is also highlighted with a red box and contains 'vrf1'. The 'Take me to this tenant when I click finish' checkbox is checked. The left sidebar shows the navigation tree with 'Tenants' selected.

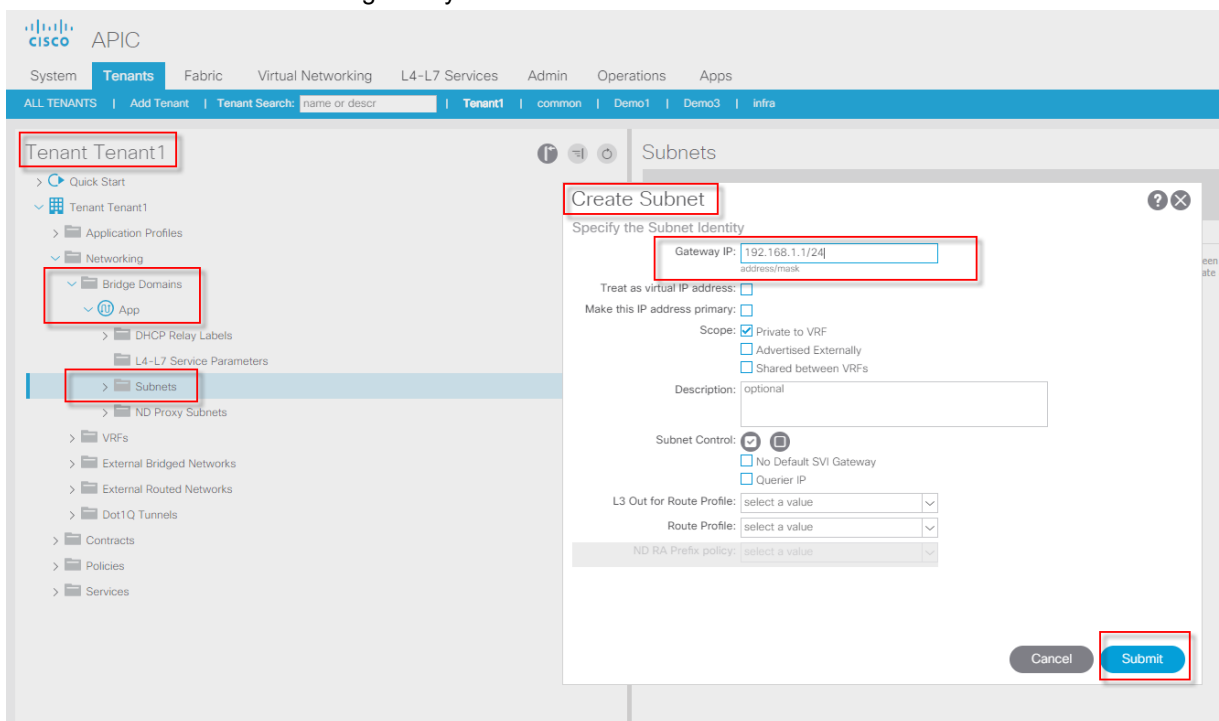
## To create a BD (app and web):

### 1. Create the app BD:

- Go to *Tenants > Tenant 1 > Networking > Bridge Domains*.
- Create the app BD as shown. In the *Name* field, enter App. From the *VRF* dropdown list, select vrf1. Click *Next*.

The screenshot shows the 'Create Bridge Domain' form in the Cisco APIC interface. The 'Name' field is highlighted with a red box and contains 'App'. The 'VRF' dropdown is highlighted with a red box and is set to 'vrf1'. The left sidebar shows the navigation tree with 'Tenant1' selected and 'Bridge Domains' highlighted. The 'Type' is set to 'regular'.

- c. Configure the other parameters as required. Click *Finish*.
2. Define a subnet gateway for the app BD:
  - a. If you are using policy base routing (PBR), this will be the gateway for the endpoints that belong to this BD. For PBR configuration, consult the Cisco configuration guide. If you are not using PBR, the endpoint gateway will be the interfaces on the FortiGate. In our example, we are using the FortiGate interface as the gateway for the endpoints. Go to the newly created BD app, then click *Subnets*.
  - b. Create the subnet and enter the gateway IP address as shown.



- c. Click *Submit*.

### 3. Create the web BD:

- a. Go to *Tenants > Tenant 1 > Networking > Bridge Domains*.
- b. Create the web BD as shown. In the *Name* field, enter web. From the *VRF* dropdown list, select vrf1. Click *Next*.

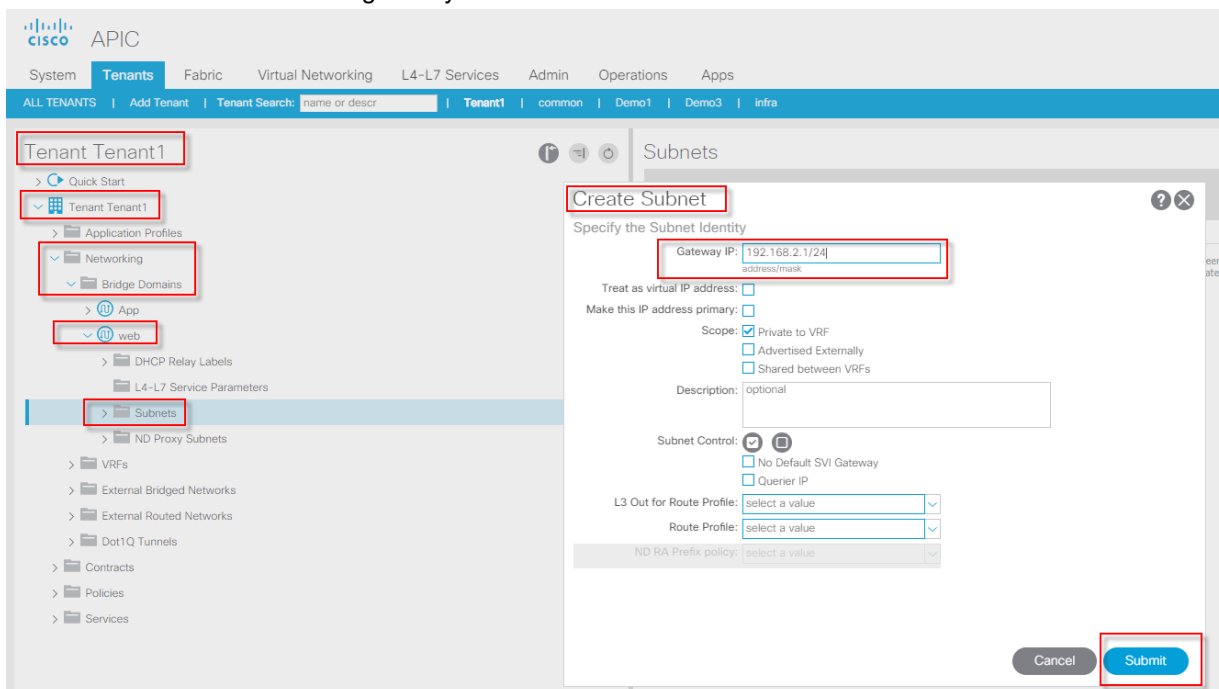
The screenshot displays the Cisco APIC interface for creating a bridge domain. The left sidebar shows the navigation tree with 'Tenant Tenant1' and 'Bridge Domains' highlighted. The main panel shows the 'Create Bridge Domain' form with the following fields and values:

- Name: web
- Alias: (empty)
- Description: optional
- Tags: (empty)
- Type: regular
- VRF: vrf1
- Forwarding: Optimize
- Endpoint Retention Policy: select a value
- IGMP Snoop Policy: select a value

The 'Next' button is visible at the bottom right of the form.

- c. Configure the other parameters as required. Click *Finish*.
- ### 4. Define a subnet gateway for the web BD:
- a. If you are using policy base routing (PBR), this will be the gateway for the endpoints that belong to this BD. For PBR configuration, consult the Cisco configuration guide. If you are not using PBR, the endpoint gateway will be the interfaces on the FortiGate. In our example, we are using the FortiGate interface as the gateway for the endpoints. Go to the newly created BD app, then click *Subnets*.

- b. Create the subnet and enter the gateway IP address as shown.

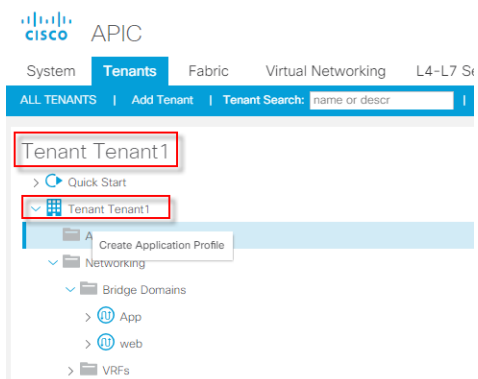


- c. Click *Submit*.

## To create EPGs:

1. Create an application profile for the EPGs:

- a. Go to *Tenants > Tenant 1 > Create Application Profile*.





- b. Configure as shown, then click **Submit**.

The screenshot shows the Cisco APIC interface. On the left, the navigation tree is expanded to 'Tenant1' > 'Application Profiles'. The main panel displays the 'Create Application Profile' dialog. The 'Name' field is set to 'AP'. Below the form, there is a table for EPGs with columns: Name, Alias, BD, Domain, Switching Mode, Static Path, Static Path VLAN, Provided Contract, and Consumed Contract. At the bottom right of the dialog, the 'Submit' button is highlighted with a red box.

2. Create the app EPG:

- Go to **Tenants > Tenant 1 > Application Profiles > AP > Application EPGs > Create Application EPG**. Do not use | in the EPG name.
- Configure as shown, selecting the web BD.
- Click **Finish**.

The screenshot shows the Cisco APIC interface. On the left, the navigation tree is expanded to 'Tenant1' > 'Application Profiles' > 'AP' > 'Application EPGs'. The main panel displays the 'Create Application EPG' dialog. The 'Name' field is set to 'app'. The 'Bridge Domain' dropdown is set to 'web'. At the bottom right of the dialog, the 'Finish' button is highlighted with a red box.

### 3. Configure tag(s) for the app EPG if desired.

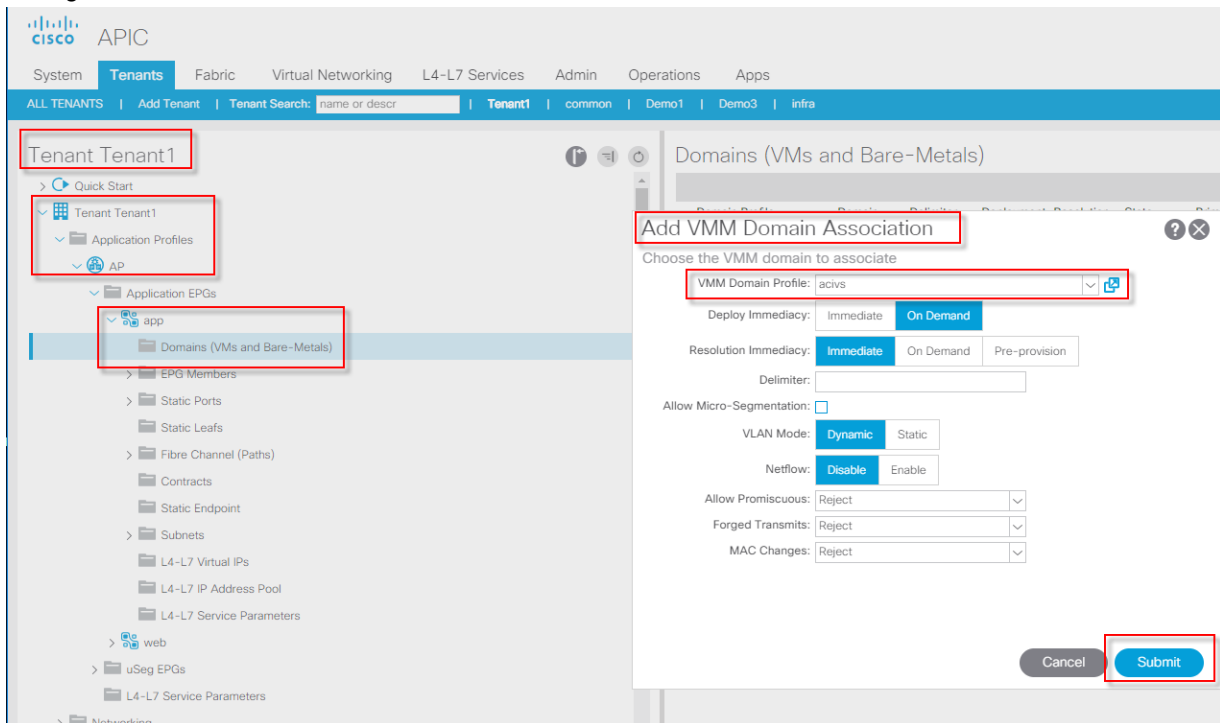
The screenshot displays the Cisco APIC interface. On the left, the navigation pane shows the hierarchy: Tenant1 > Application Profiles > AP > Application EPGs > app. The main pane shows the configuration for 'EPG - app'. The 'General' tab is selected, and the 'Tags' field is configured with the value 'r/APP-200'.

### 4. Map endpoint VMs to the app EPG:

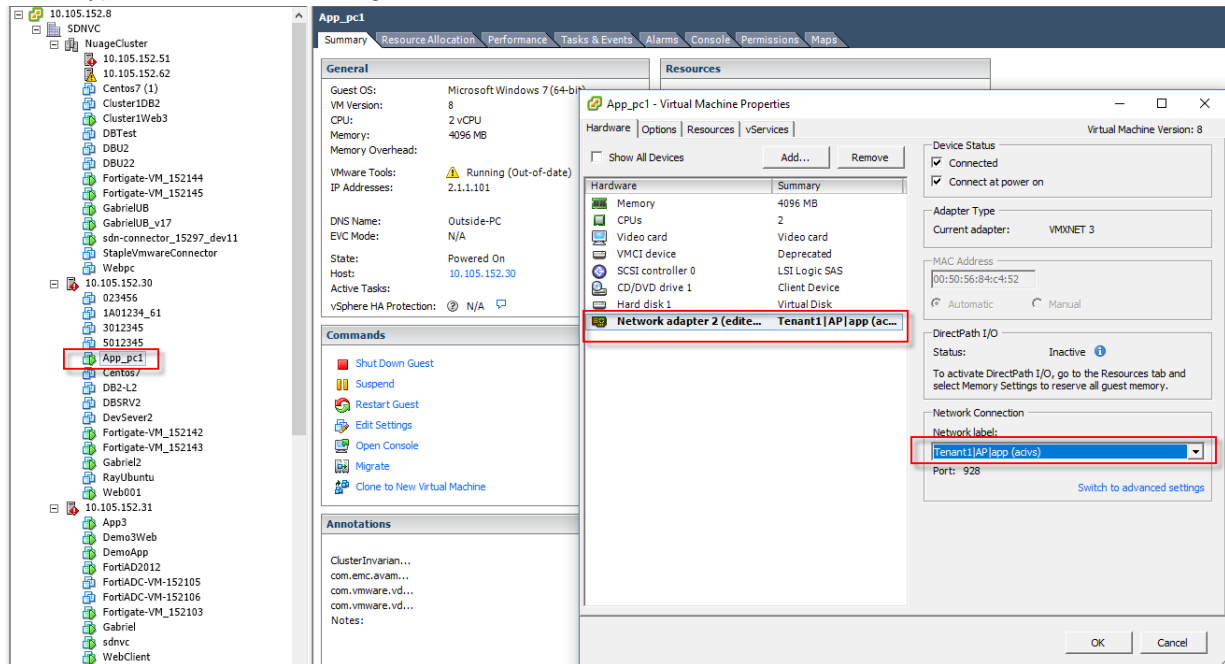
- a. Go to **Tenants > Tenant1 > Application Profiles > AP > Application EPGs > app**, then right-click **Domains (VMs and Bare-Metals)**. Select **Add VMM Domain Association**.

The screenshot shows the same navigation path as the previous image. The 'Domains (VMs and Bare-Metals)' item is right-clicked, and a context menu is displayed with the following options: 'Add VMM Domain Association', 'Add Physical Domain Association', 'Add L2 External Domain Association', and 'Add Fibre Channel Domain Association'.

- b. Configure the VMM domain association as shown. Click **Submit**.



- c. In the hypervisor, select the configured VMM domain association under the **Network** label.



5. Repeat step b to create the web EPG, selecting the web BD instead of the app BD. Do not use | in the EPG name.

The screenshot shows the Cisco APIC interface for creating an Application EPG. The left sidebar displays the navigation tree with 'Tenant Tenant1' and 'Application EPGs' highlighted. The main form is titled 'Create Application EPG' and 'STEP 1 > Identity'. It contains the following fields and options:

- Name: web
- Alias: (empty)
- Description: optional
- Tags: (empty)
- Contract Exception Tag: (empty)
- QoS class: Unspecified
- Custom QoS: select a value
- Data-Plane Policer: select a value
- Intra EPG Isolation: Unenforced
- Preferred Group Member: Exclude
- Flood on Encapsulation: Disabled
- Bridge Domain: web
- Monitoring Policy: select a value
- FHS Trust Control Policy: select a value
- Associate to VM Domain Profiles: ☐
- Statically Link with Leaves/Paths: ☐
- EPG Contract Master: (empty)

The 'Finish' button is highlighted in red.

6. If desired, create tag(s) for the web EPG.  
7. Repeat step c to map endpoints to the web EPG.

#### To create an L4-L7 device:

1. Go to *Tenant > Tenant1 > Services > L4-L7 > Devices > Create L4-L7 Devices*.
2. If using unmanaged mode, ensure that the *Managed* checkbox is not selected.

### 3. Configure as shown, then click *Finish*.

**Create L4-L7 Devices**

STEP 1 > General

Select device package and specify connectivity

General

Managed: ☐ (Make sure this is unchecked for Unmanaged mode)

Name: FGT1

Service Type: Firewall

Device Type: PHYSICAL VIRTUAL

Physical Domain: FWDomain

View: Single Node HA Node

Promiscuous Mode: ☐

Context Aware: Multiple Single

Function Type: GoThrough GoTo

Device 1

Device Interfaces:

Name	Path
port5	Pod-1/Node-103/eth1/9
port6	Pod-1/Node-103/eth1/10

Cluster

Cluster Interfaces:

Name	Concrete Interfaces	Encap
consumer	Device1/port5	
provider	Device1/port6	

Previous Cancel **Finish**

### To create the service graph template:

1. Go to *Tenant > Tenant1 > Services > L4-L7 > Service Graph Templates > Create L4-L7 Service Graph Template*.
2. Configure the service graph template.
3. Click *Submit*.

**Create L4-L7 Service Graph Template**

Drag device clusters to create graph nodes:

Device Clusters

svcType: FW

Tenant1/FGT1

Service Graph Name: Template1

Graph Type: Create a New Graph Clone an Existing Graph

Consumer EPG

FGT1

Provider EPG

FGT1 Information

Firewall: Routed Transparent

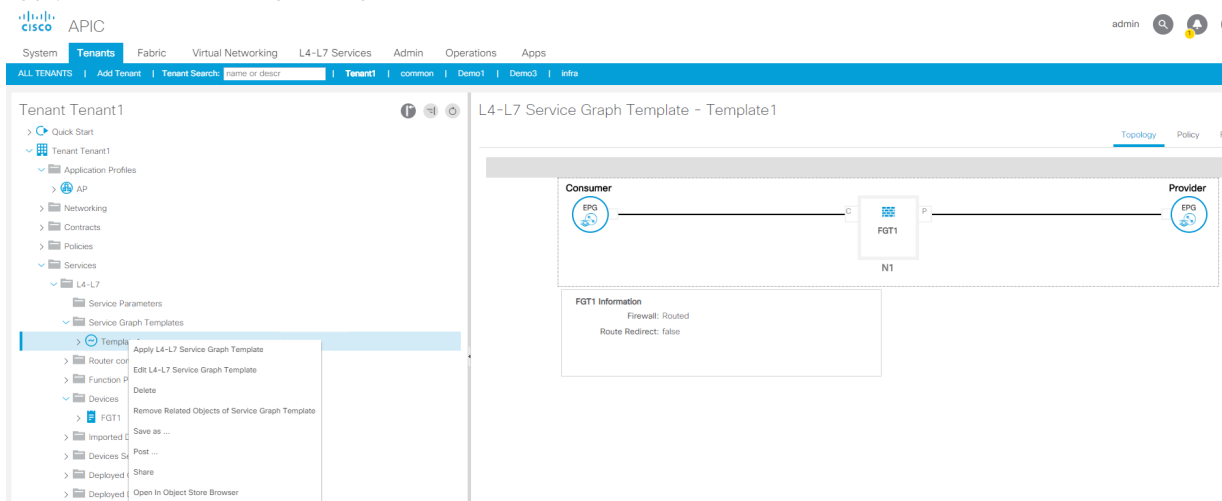
Route Redirect: ☐

Cancel **Submit**

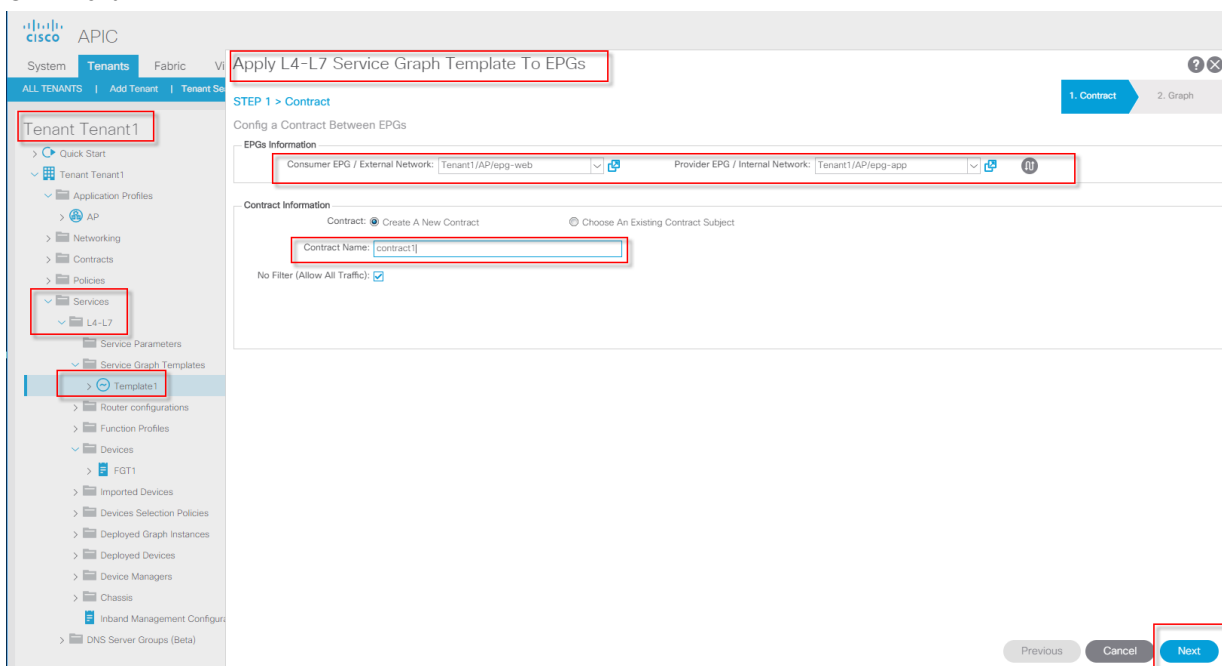
## To deploy the service graph template between the web and app EPGs:

### 1. Deploy the service graph between the web and app EPGs:

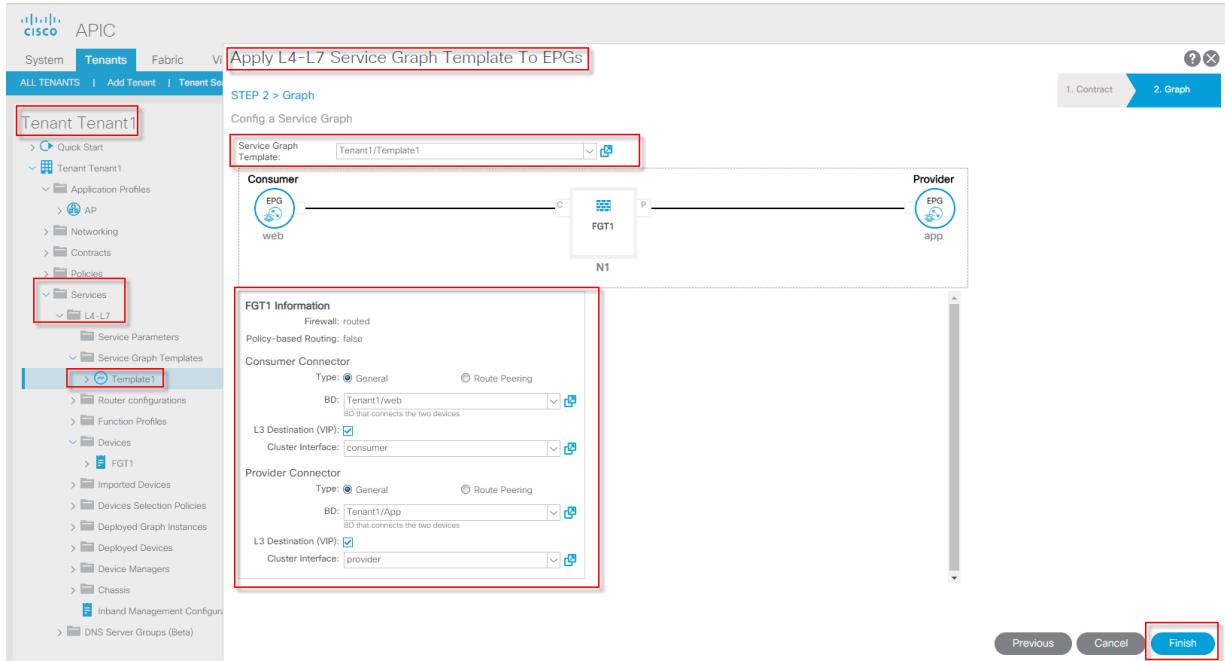
- a. Go to **Tenant > Tenant1 > Services > L4-L7 > Service Graph Templates**. Right-click **Template1**, then select **Apply L4-L7 Service Graph Template**.



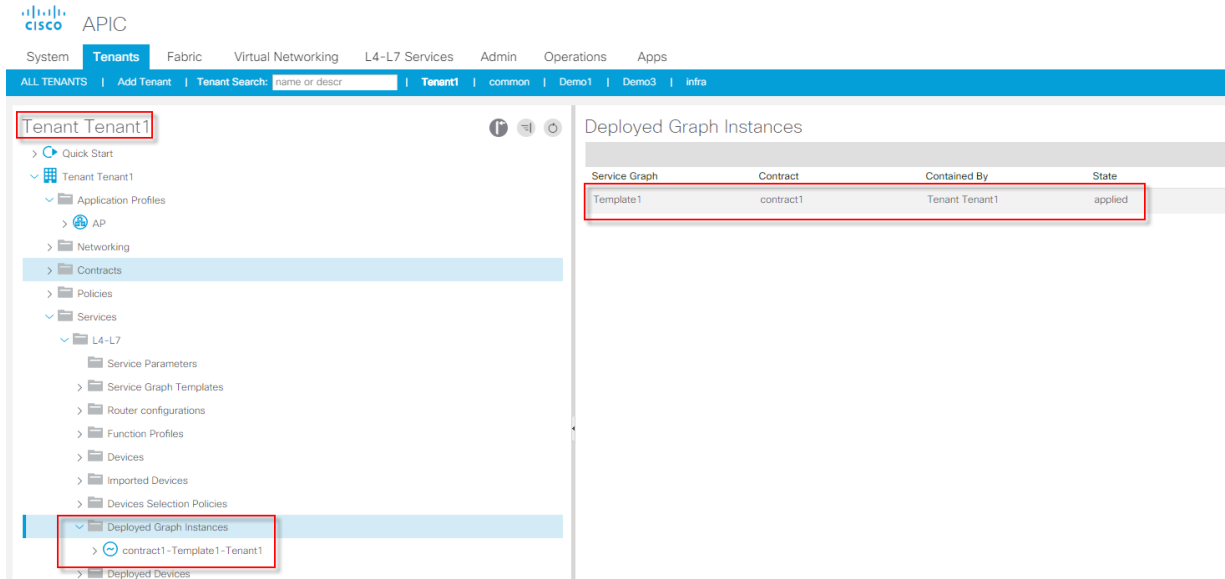
- b. From the **Consumer EPG / External Network** dropdown list, select the web EPG.
- c. From the **Provider EPG / Internal Network** dropdown list, select the app EPG.
- d. Enter a contract name.
- e. Click **Next**.



- f. From the **Service Graph Template** dropdown list, select the service graph template configured in step h.
- g. Under **FGT1 Information**, configure the consumer connector as shown, selecting the web BD. Configure the provider connector with the app BD.



h. Click *Finish*. The service graph is deployed.



2. Obtain the VLANs assigned to the interfaces. You will configure the corresponding VLANs on the FortiGate side:
  - a. Go to *Tenant > Tenant1 > Services > L4-L7 > Deployed Graph Instances > contract1-Template1-Tenant1 > Function Node - N1*.

- b. Under *Function Connectors*, note the VLANs listed for the consumer and provider in the *Encap* column.

The screenshot displays the FortiGate GUI configuration for a Function Node. The left sidebar shows the navigation tree with 'Tenant1' selected. The main panel shows the 'Function Node - N1' configuration. The 'Cluster Interfaces' table shows 'consumer' and 'provider' interfaces. The 'Function Connectors' table shows 'consumer' and 'provider' connectors with their respective 'Encap' values (vlan-2767 and vlan-2766). The 'Folders And Parameters' section shows a table with 'Meta Folder/Param Key', 'Name', 'Value', and 'Override name/value To'.

## Deploying SDN Connector

SDN Connector works with standalone FortiGate as well as FortiManager. The below sections describe steps for deploying FortiGate in standalone or managed mode with FortiManager:

- [Deploying SDN Connector with FortiGate \(standalone\) on page 40](#)
- [Deploying SDN Connector with FortiManager on page 46](#)

### Deploying SDN Connector with FortiGate (standalone)

Deploying SDN Connector when using FortiGate in standalone mode consists of the following steps:

1. Create a VDOM.
2. Create VLAN interfaces.
3. Create static routes.
4. Configure a Fabric SDN Connector.
5. Create dynamic addresses.
6. Create policies using the dynamic address(es).

#### To create a VDOM:

1. In FortiOS, connect to the management VDOM.
2. Go to *Global > System > VDOM* and select *Create New*.
3. Enter a unique *Name*. VDOM names have the following restrictions:
  - Only letters, numbers, "-", and "\_" are allowed.
  - No more than eleven characters are allowed.
  - No spaces are allowed.
  - VDOMs cannot have the same names as interfaces, zones, switch interfaces, or other VDOMs.
4. Enter a short and descriptive comment to identify this VDOM.
5. Select *OK*.



### To create VLAN interfaces:

1. Go to *Network > Interfaces*.
2. Click *Create New > Interface*.
3. Configure an interface for each VLAN noted in the last step of [Cisco ACI deployment on page 28](#). Ensure that the VLAN mapped to the interface corresponds to the VLAN that ACI assigned during service graph deployment.

FortiGate 3700D FGT37D4615800597

Global > New

Interface Name: port5\_vlan2767

Alias:

Type: VLAN

Interface: port5

VLAN ID: 2767

Virtual Domain: NYC

Tags

Role: LAN

Address

Addressing mode: Manual DHCP

IP/Network Mask: 192.168.2.2/24

IPv6 Addressing mode: Manual DHCP

IPv6 Address/Prefix: ::0

Administrative Access

IPv4

☒ HTTPS ☒ HTTP ☒ PING ☐ FMG-Access

☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM

☐ RADIUS Accounting ☐ FortiTelemetry

IPv6 Administrative Access

☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access

☐ CAPWAP ☐ SSH ☐ SNMP ☐ FTM

☐ DHCP Server

Networked Devices

Device Detection: ☒

Active Scanning: ☐

OK Cancel

**FortiGate 3700D** FGT37D4615800597

Global | Dashboard | Security Fabric | **Network** | **Interfaces** | DNS | System | Policy & Objects | Security Profiles | Log & Report

New

Interface Name: port\_vlan2766  
 Alias:   
 Type: VLAN  
 Interface: port6  
 VLAN ID: 2766  
 Virtual Domain: NYC

Tags  
 Role: LAN  
 Add Tag Category

Address  
 Addressing mode: Manual DHCP  
 IP/Network Mask: 192.168.1.2/24  
 IPv6 Addressing mode: Manual DHCP  
 IPv6 Address/Prefix: ::/0

Administrative Access  
 IPv4: ☒ HTTPS ☒ HTTP ☒ PING ☐ FMG-Access  
☐ CAPWAP ☒ SSH ☐ SNMP ☐ FTM  
☐ RADIUS Accounting ☐ FortiTelemetry  
 IPv6 Administrative Access: ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access  
☐ CAPWAP ☐ SSH ☐ SNMP ☐ FTM

☐ DHCP Server

Networked Devices  
 Device Detection: ☒  
 Active Scanning: ☐

OK Cancel

### To create static routes:

1. Go to *Network > Static Routes*.
2. Click *Create New*.
3. Configure two static routes as shown below: one for each VLAN configured in the previous section.

**FortiGate 3700D** FGT37D4615800597

NYC | + Create New | Edit | Clone | Delete

Destination	Gateway	
IPv4 (2)		
192.168.2.0/24	192.168.2.1	port5_vlan2767
192.168.1.0/24	192.168.1.1	port6_vlan2766

Static Routes

### To configure an SDN connector:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. Under *SDN*, select *Application Centric Infrastructure (ACI)*.

4. Configure the SDN Connector, then click OK. The default port is 5671.

FortiGate 3700D FGT37D4615800597

Global

New Fabric Connector

SDN

Application Centric Infrastructure (ACI)

Connector Settings

Name: SDNConnector

IP: 10.105.152.97

Port: Use Default Specify

Username: admin

Password: [masked]

Status: On

OK Cancel

#### To create dynamic addresses:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Configure a dynamic address for the app EPG. Ensure that the format for the endpoint group name is entered as "Application Profile name|EPG name". This is case-sensitive. In [Cisco ACI deployment on page 28](#), the application profile was named "AP", and the EPGs were named "app" and "web". Therefore, the correct format is AP|app and AP|web, as shown below.

FortiGate 3700D FGT37D4615800597

NYC

New Address

Category: Address IPv6 Address

Name: WebEPG

Color: Change

Type: Fabric Connector Address

Fabric Connector Type: Application Centric Infrastructure (ACI)

Tenant: Tenant1

Endpoint Group Name: AP|web

Tag: TAG-100

Interface: any

Show in Address List: On

Comments: 0/255

Tags: Add Tag Category

OK Cancel

#### 4. Repeat steps 2 and 3 to configure a dynamic address for the web EPG.

FortiGate 3700D FGT37D4615800597

NYC

New Address

Category: Address IPv6 Address

Name: AppEPG

Color: Change

Type: Fabric Connector Address

Fabric Connector Type: Application Centric Infrastructure (A

Tenant: Tenant1

Endpoint Group Name: AP|app

Tag: TAG-200

Interface: any

Show in Address List: ☒

Comments: 0/255

Tags: Add Tag Category

OK Cancel

The following shows that the FortiOS and SDN Connector output regarding the web and app EPGs contain corresponding information:

```
FGT37D4615800597 (NYC) # diag firewall dynamic list
List all SDN dynamic addresses:
ac1.Tenant1.AP|web.TAG-100: ID(55) REF(1) ADDR(192.168.2.10)
ac1.Tenant1.AP|app.TAG-200: ID(59) REF(1) ADDR(192.168.1.10)
ac1.Demo2.AP|web01.*: ID(68) REF(1) ADDR(1.1.1.10)
ac1.Demo2.LongEPGName0123456789012345678901234567890123456789012.*: ID(89) REF(1) ADDR(2.1.1.100)
ac1.Demo2.AP|LongEPGName0123456789012345678901234567890123456789012.*: ID(102) REF(1) ADDR(2.1.1.100)
ac1.Demo2.AP2|LongEPGName0123456789012345678901234567890123456789012.*: ID(152) REF(1)
ac1.Demo2.LongEPGName0123456789012345678901234567890123456789012.TAG-55: ID(162) REF(1)
ac1.Demo2.*.*: ID(194) REF(1) ADDR(1.1.1.10) ADDR(2.1.1.10) ADDR(2.1.1.100)
ac1.Demo2.AP|LongEPGName0123456789012345678901234567890123456789012.TAG-100: ID(214) REF(1)
```

Fortinet SDN Connector

Configuration

Running Status

Cache Content

Download Log

UpgradeService

RestartService

ChangePassword

Logout

DN	TAGS	Dynamic Address List	Address Count
tn-Demo2/ap-AP/epg-app01	[]	[{"ip":"2.1.1.10","mac":"00:50:56:22:22:22"}]	1
tn-Demo2/ap-AP/epg-LongEPGName0123456789012345678901234567890123456789012	[{"number_2000"}]	[{"ip":"2.1.1.100","mac":"00:50:56:84:6F:80"}]	1
tn-Demo2/ap-AP/epg-web01	[]	[{"ip":"1.1.1.10","mac":"00:50:56:B4:F5:BC"}, {"ip":"1.1.1.10","mac":"00:50:56:84:7C:51"}]	2
tn-Demo3/ap-AP/epg-web01	[]	[{"ip":"4.1.1.10","mac":"00:50:56:11:11:11"}]	1
tn-t1/ap-ap/epg-App_2	[{"TAG-34","TAG-23","TAG-20","TAG-28","TAG-54","test-tag200","johnsonitag","TAG-13","TAG-81","TAG-49"}]	[{"ip":"10.26.10.3","mac":"54:7F:EE:29:50:BC"}]	1
tn-Tenant1/ap-AP/epg-app	[{"TAG-200"}]	[{"ip":"192.168.1.10","mac":"00:50:56:84:C4:52"}]	1
tn-Tenant1/ap-AP/epg-web	[{"TAG-100"}]	[{"ip":"192.168.2.10","mac":"00:50:56:84:3E:1F"}]	1
tn-test1/ap-AP/epg-app01	[]	[{"ip":"192.168.20.10","mac":"00:50:56:B4:FE:46"}]	1

Previous

1

Next

Total DN with endpoints: 8

#### To create policies using the dynamic addresses:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*.

3. Create a policy that allows communication from the web EPG to the app EPG as shown:

The screenshot shows the FortiGate 3700D configuration interface. The left sidebar has a menu with 'IPv4 Policy' highlighted. The main area displays the 'New Policy' dialog box. The dialog box has the following fields:

- Name: WebtoApp
- Incoming Interface: port5\_vlan2767
- Outgoing Interface: port6\_vlan2766
- Source: WebEPG
- Destination: AppEPG
- Schedule: always
- Service: ALL
- Action: ACCEPT (checked), DENY (unchecked)

Below the dialog box, there are sections for 'Firewall / Network Options', 'Security Profiles', and 'Logging Options'. The 'Logging Options' section shows 'Log Allowed Traffic' checked, 'Generate Logs when Session Starts' unchecked, and 'Capture Packets' unchecked. The 'OK' button is highlighted in green.

4. Create a policy that allows communication from the app EPG to the web EPG as shown:

The screenshot shows the FortiGate 3700D configuration interface. The left sidebar is expanded to 'Policy & Objects' > 'IPv4 Policy'. The 'New Policy' dialog is open, showing the following configuration:

- Name:** ApptoWeb
- Incoming Interface:** port6\_vlan2766
- Outgoing Interface:** port5\_vlan2767
- Source:** AppEPG
- Destination:** WebEPG
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)

Below the policy configuration, the 'Firewall / Network Options' section is visible, including NAT, Proxy Options, Security Profiles (AntiVirus, Web Filter, DNS Filter, Application Control, IPS, SSL Inspection), and Logging Options (Log Allowed Traffic, Generate Logs when Session Starts, Capture Packets).

5. Ensure that an endpoint in the web EPG and an endpoint in the app EPG can ping each other.

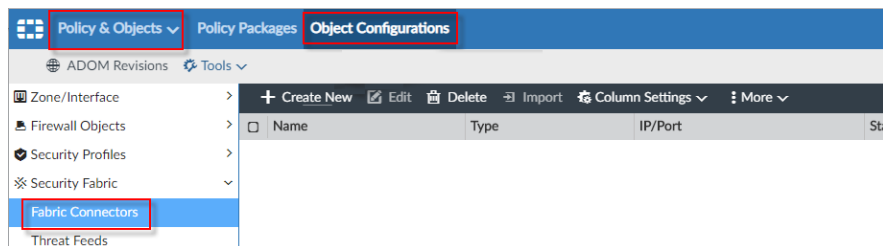
## Deploying SDN Connector with FortiManager

Deploying SDN Connector when using FortiManager consists of the following steps:

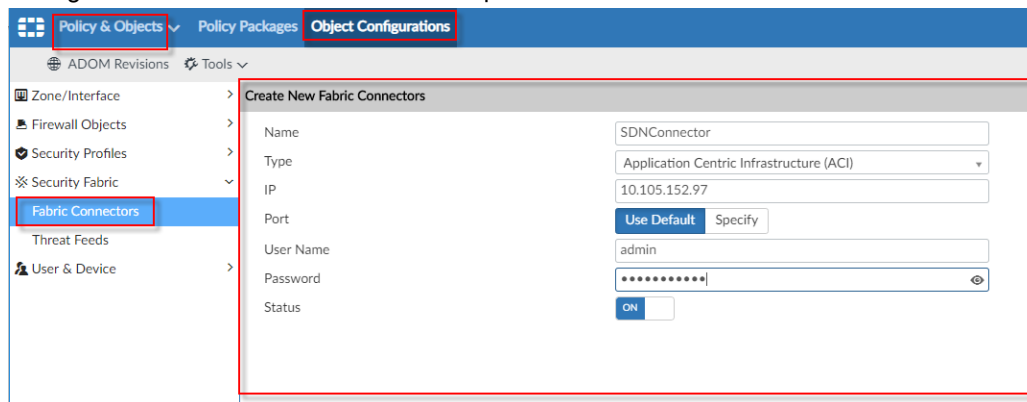
1. Configure a Fabric SDN Connector.
2. Create or import address objects.
3. Map the web and app interfaces.
4. Create policies leveraging the address objects.
5. Push the configuration to the FortiGate.

### To configure a Fabric SDN Connector:

1. In FortiManager, go to *Policy & Objects > Security Fabric > Fabric Connectors*.
2. Click *Create New*.



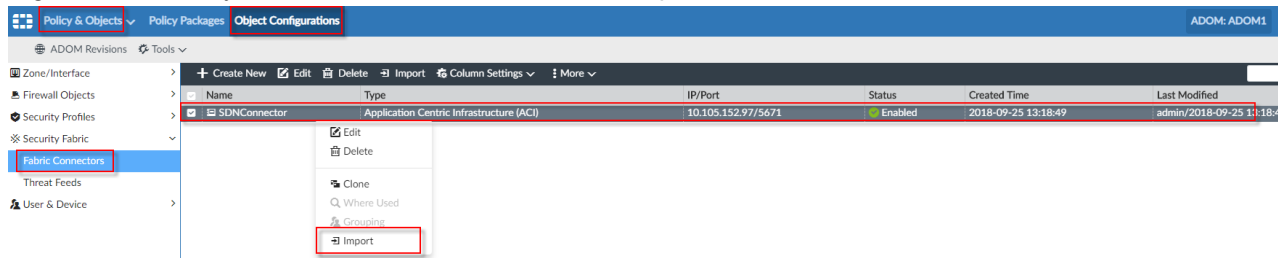
3. Configure the SDN Connector. The default port is 5671.



### To create or import address objects:

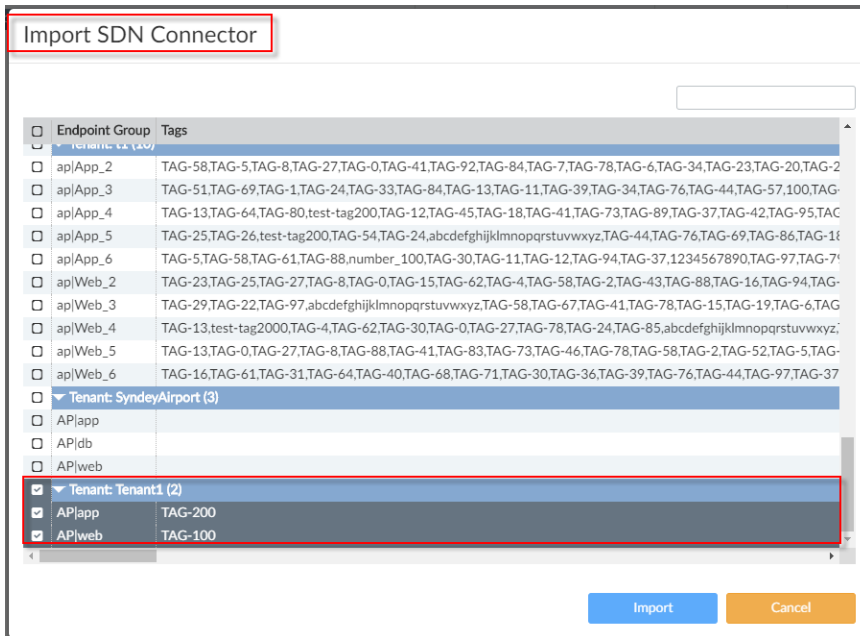
To import address objects, do the following:

1. Go to *Policy & Objects > Security Fabric > Fabric Connectors*.
2. Right-click the newly created SDN Connector and select *Import* from the context menu.



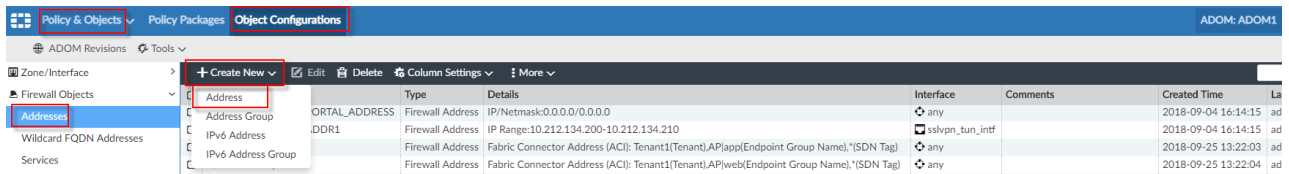
3. In the *Import SDN Connector* dialog, select the EPGs to import. In this example, the AP|app and AP|web EPGs are

imported.



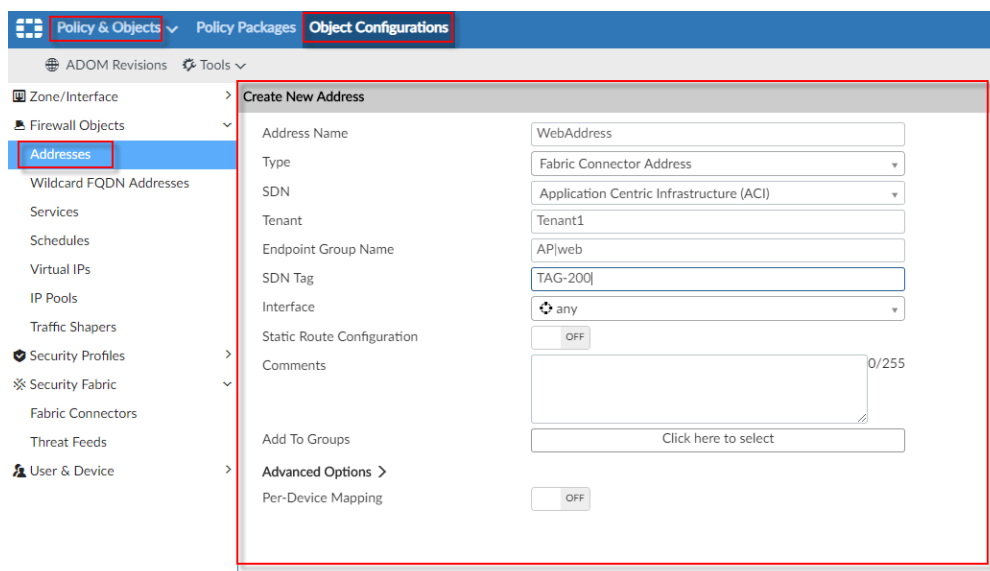
To manually create address objects, do the following:

1. Go to **Policy & Objects > Firewall Objects > Addresses**.
2. Click **Create New > Address**.



3. Configure a dynamic address for the web EPG. Ensure that the format for the endpoint group name is entered as "Application Profile name|EPG name". This is case-sensitive. In [Cisco ACI deployment on page 28](#), the application profile was named "AP", and the EPGs were named "app" and "web". Therefore, the correct format is AP|app and AP|web, as shown below.





**Policy & Objects** Policy Packages **Object Configurations**

ADOM Revisions Tools

**Zone/Interface**

**Addresses**

Wildcard FQDN Addresses

Services

Schedules

Virtual IPs

IP Pools

Traffic Shapers

Security Profiles

Security Fabric

Fabric Connectors

Threat Feeds

User & Device

**Create New Address**

Address Name: WebAddress

Type: Fabric Connector Address

SDN: Application Centric Infrastructure (ACI)

Tenant: Tenant1

Endpoint Group Name: AP|web

SDN Tag: TAG-200

Interface: any

Static Route Configuration: OFF

Comments: 0/255

Add To Groups: Click here to select

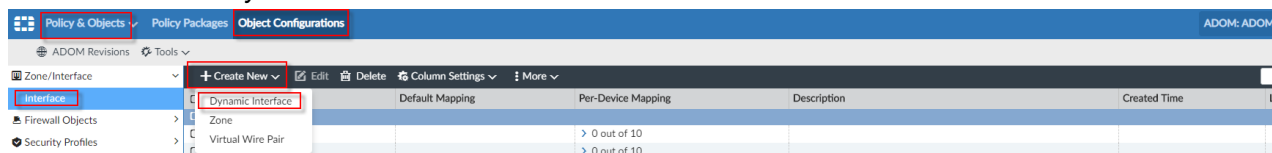
Advanced Options >

Per-Device Mapping: OFF

- Repeat steps 2 and 3 to configure a dynamic address for the app EPG.

### To map the web and app interfaces:

- Go to *Policy & Objects > Zone/Interface > Interface*.
- Click *Create New > Dynamic Interface*.



**Policy & Objects** Policy Packages **Object Configurations** ADOM: ADOM1

ADOM Revisions Tools

**Zone/Interface**

**Interface**

Dynamic Interface

Default Mapping

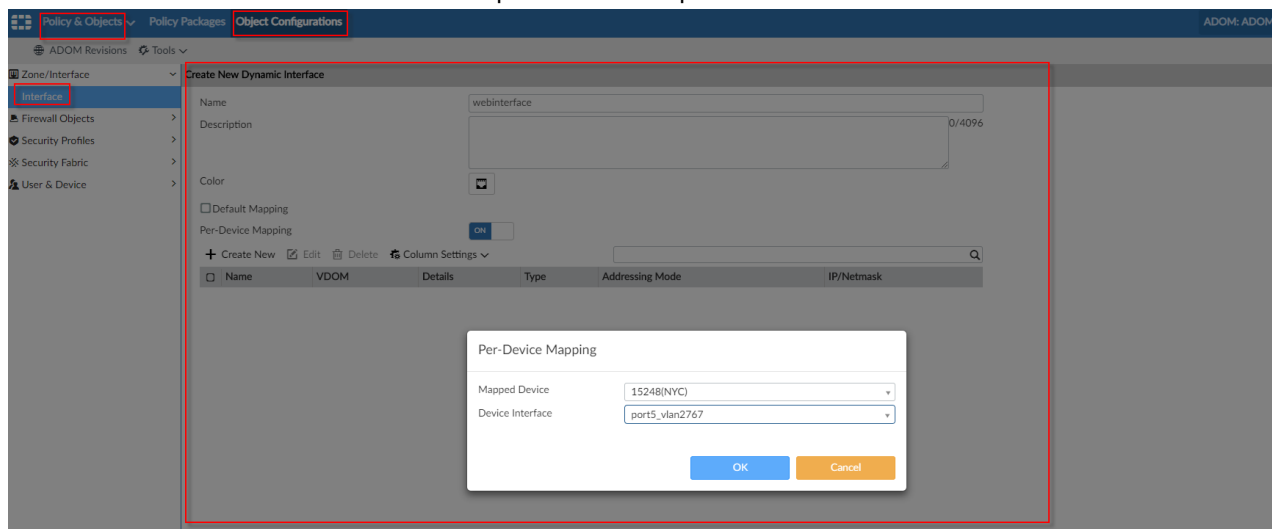
Per-Device Mapping

Description

Created Time

Las

- Create an interface for the web EPG that maps to the correct port and VLAN.



**Policy & Objects** Policy Packages **Object Configurations** ADOM: ADOM1

ADOM Revisions Tools

**Zone/Interface**

**Interface**

Create New Dynamic Interface

Name: webinterface

Description: 0/4096

Color: blue

Default Mapping: OFF

Per-Device Mapping: ON

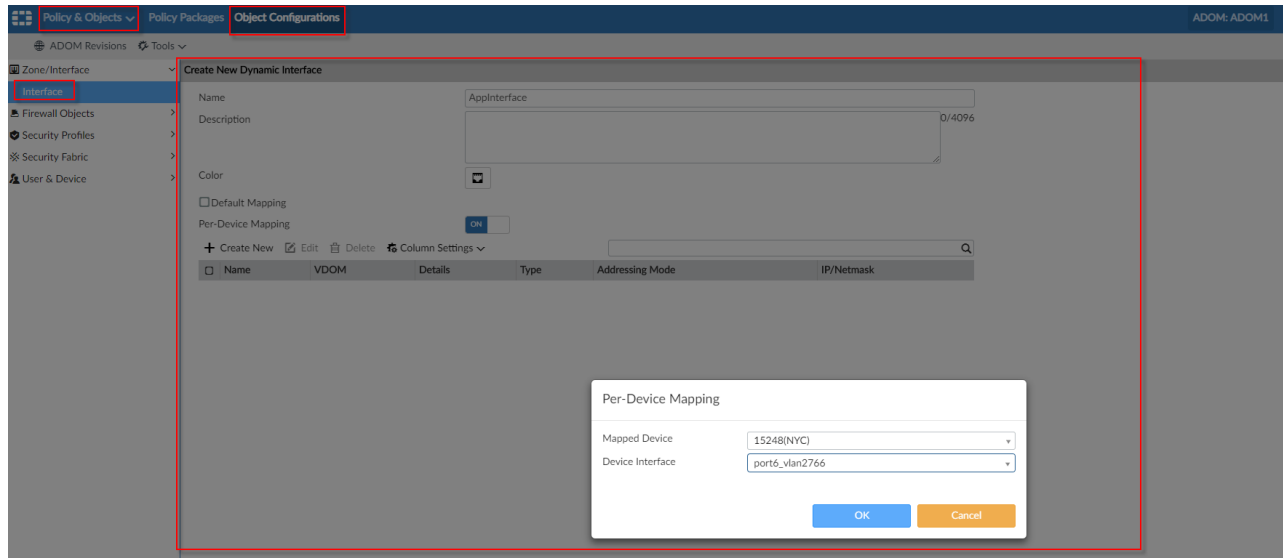
Per-Device Mapping

Mapped Device: 15248(NYC)

Device Interface: port5\_vlan2767

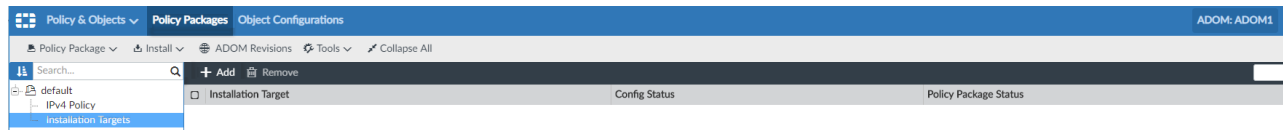
OK Cancel

#### 4. Repeat step 3 for the app EPG.

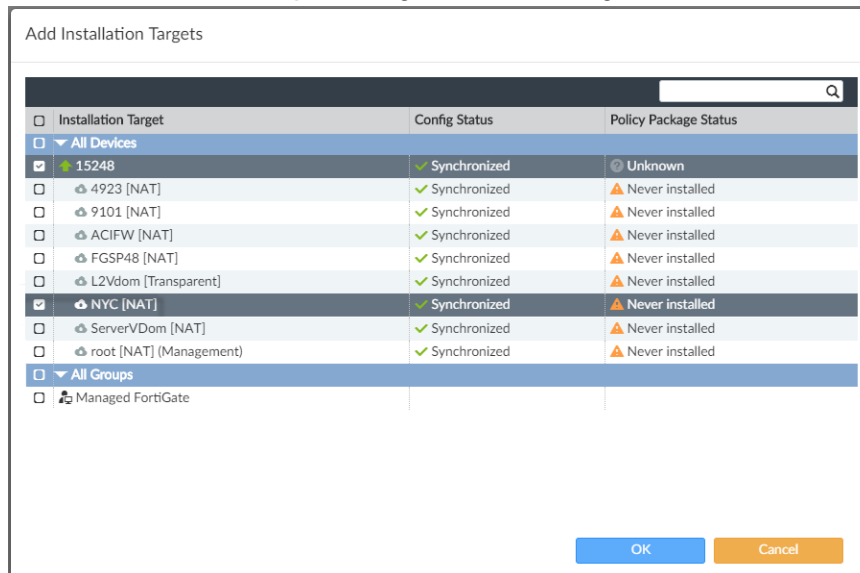


#### To create policies leveraging the address objects:

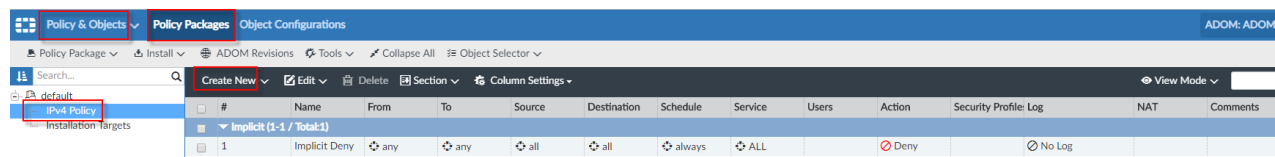
1. Go to *Policy & Objects > Policy Packages > default > Installation Targets*.
2. Click **Add**.



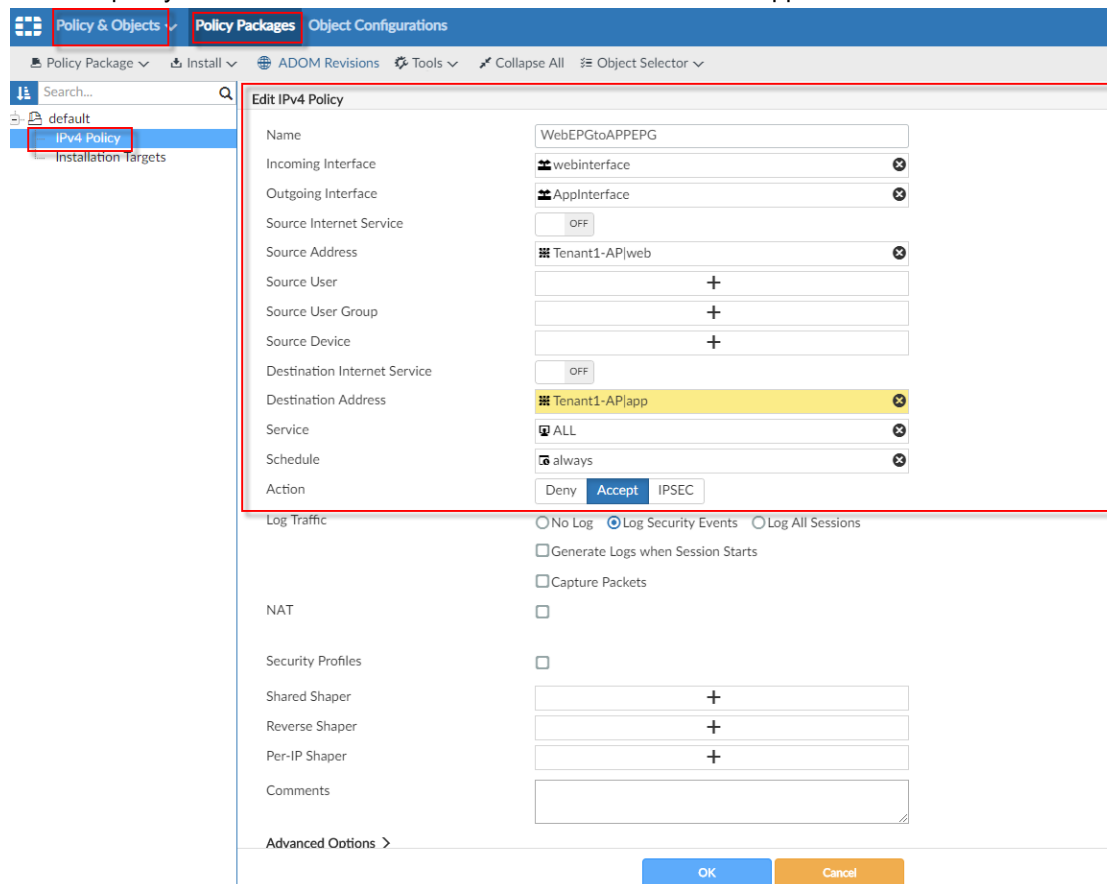
3. In the *Add Installation Targets* dialog, select the managed FortiGate. Click **OK**.



4. Go to *Policy & Objects > Policy Packages > default > IPv4 Policy*.

5. Click *Create New*.

## 6. Create a policy that allows communication from the web EPG to the app EPG as shown:



7. Create a policy that allows communication from the app EPG to the web EPG as shown:

**Policy & Objects** | **Policy Packages** | Object Configurations

Policy Package | Install | ADOM Revisions | Tools | Collapse All | Object Selector

Search...

default

IPv4 Policy

Installation Targets

**Edit IPv4 Policy**

Name: AppEPGtoWebEPG

Incoming Interface: AppInterface

Outgoing Interface: webinterface

Source Internet Service: OFF

Source Address: Tenant1-AP|app

Source User: +

Source User Group: +

Source Device: +

Destination Internet Service: OFF

Destination Address: Tenant1-AP|web

Service: ALL

Schedule: always

Action: Deny | **Accept** | IPSEC

Log Traffic: ☐ No Log | ☒ Log Security Events | ☐ Log All Sessions

☐ Generate Logs when Session Starts

☐ Capture Packets

NAT: ☐

Security Profiles: ☐

Shared Shaper: +

Reverse Shaper: +

Per-IP Shaper: +

Comments:

Advanced Options >

OK Cancel

**To push the configuration to the FortiGate:**

1. Go to *Policy & Objects > Policy Packages > default > IPv4 Policy*.
2. Click *Install > Install Wizard*.

**Policy & Objects** | **Policy Packages** | Object Configurations

Policy Package | Install | ADOM Revisions | Tools | Collapse All | Object Selector

Search...

default

IPv4 Policy

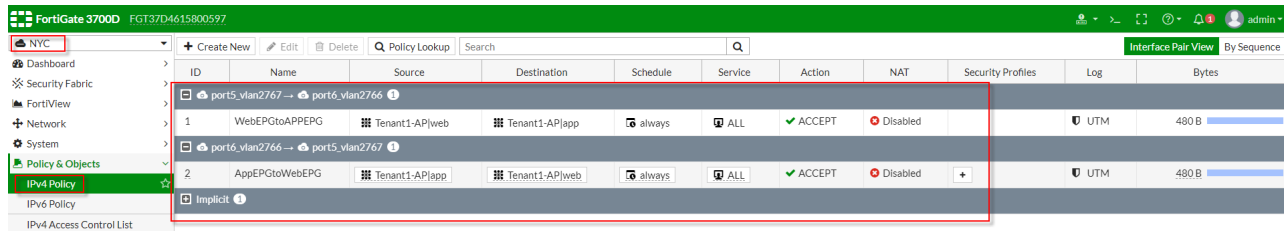
Installation Targets

**Install Wizard**

Re-install Policy

Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile	Log	NAT	Comments
1	WebEPGtoAPP	webinterface	AppInterface	Tenant1-AP	Tenant1-AP	always	ALL	Accept	Log Security Events	Disabled		
2	AppEPGtoWeb	AppInterface	webinterface	Tenant1-AP	Tenant1-AP	always	ALL	Accept	Log Security Events	Disabled		
<b>Implicit (3-3 / Total:1)</b>												
3	Implicit Deny	any	any	all	all	always	ALL	Deny	No Log			

3. In the Install Wizard, ensure that the default policy package is selected. Click *Next*.
4. Select the managed FortiGate. Click *Next*.
5. Ensure that the summary is correct, then click *Install*.
6. When installation is complete, click *Finish*.
7. In FortiOS, go to *Policy & Objects > IPv4 Policy* to ensure that the policies were pushed and are configured as desired.



8. Ensure that an endpoint in the web EPG and an endpoint in the app EPG can ping each other.

## Monitoring SDN connector status using an API

You can monitor SDN connector status using a REST API that Fortinet SDN Connector for Cisco ACI and Nuage Networks provides.

### Request:

/api/status

### Response:

Format: json

Key	Type	Possible values	Description
in_sync	Boolean	<ul style="list-style-type: none"> <li>true</li> <li>false</li> </ul>	Whether endpoints are synchronized with upstream SDN controller.
rpc_listener	String	<ul style="list-style-type: none"> <li>connected</li> <li>disconnected</li> <li>uninitialized</li> </ul>	<p>Send and receive notifications to and from FortiOS and FortiManager.</p> <ul style="list-style-type: none"> <li>connected: SDN connector connected to RabbitMQ for receiving and sending notifications</li> <li>disconnected: connection to RabbitMQ is down.</li> <li>uninitialized: SDN connector has not initialized connection with RabbitMQ yet, during startup stage</li> </ul>
sdn_controller	String	<ul style="list-style-type: none"> <li>connected</li> <li>disconnected</li> </ul>	<p>Controller that the SDN connector connects to in order to get endpoint updates.</p> <ul style="list-style-type: none"> <li>connected: SDN connector connection to SDN controller is successful.</li> <li>disconnected: SDN connector connection to SDN controller fails due to outage or invalid username/password or has not completed yet.</li> </ul>
sdn_controller_host	String	<ul style="list-style-type: none"> <li>IP address</li> <li>FQDN</li> </ul>	IP address or FQDN of the SDN controller that the SDN connector is connecting to.
type	String	<ul style="list-style-type: none"> <li>aci</li> <li>nuage</li> </ul>	Current SDN controller type.

Key	Type	Possible values	Description
time	Integer	Epoch time in seconds	Current epoch time stamp.
usage	Dictionary		
usage.cpu	Float	0-100	SDN connector CPU usage.
usage.mem	Float	0-100	SDN connector memory usage.
version	String	x.x.x	Version number in major.minor.patch format.

The following is an example of the output:

```
{
  "in_sync": true,
  "rpc_listener": "connected",
  "sdn_controller": "connected",
  "sdn_controller_host": "x.x.x.x",
  "time": 1584398898,
  "type": "aci",
  "usage": {
    "cpu": 7.6,
    "mem": 69.7
  },
  "version": "1.1.3"
}
```

The following shows sample code for monitoring the SDN connector using this API:

```
#!/usr/bin/env python
import re
import requests

class SdnConnectorClient(object):

    def __init__(self, host, password, user="admin@sdn-connector.local"):
        self.host = host
        self.base_url = "https://" + host
        self.user = user
        self.password = password
        self.csrf = None
        self.cookies = None

    def login(self):
        login_page = requests.get(self.base_url + '/login', verify=False)
        session = login_page.cookies
        regex = re.compile(".+csrf_token=\\'(\S+)\\'(.+)"
        self.csrf = regex.search(login_page.text).group(1)
        form = {"email": self.user, "password": self.password,
               "csrf_token": self.csrf, "submit": "Login", "next": "/" }
        res = requests.post(self.base_url + '/login', data=form,
                           verify=False, cookies=session,
                           headers={'referer': self.base_url})
        self.cookies = res.cookies

    def get_status(self):
```

```

        res = self.get('/api/status')
        return res[1]

    def get(self, path):
        res = requests.get(self.base_url + path, cookies=self.cookies,
                           verify=False)
        return res.status_code, res.text

    def post(self, path, data):
        res = requests.post(self.base_url + path, cookies=self.cookies,
                            data=data, verify=False)
        return res.status_code, res.text

if __name__ == "__main__":
    sdn_client = SdnConnectorClient('localhost', 'xxxxxx')
    sdn_client.login()
    print sdn_client.get_status()

```

## FortiGate built-in connector

You can use the Cisco ACI (Application Centric Infrastructure) connector for northbound API integration with a direct connection.

Multiple server IP addresses can be included for the Cisco APIC cluster active and standby hosts. One server is active, and the rest serve as backups in case the active server fails. The FortiGate checks the status of the servers, and selects one as the active server according to the order of the IP addresses in the list. If the active server fails, the FortiGate changes to the next one down on the list.

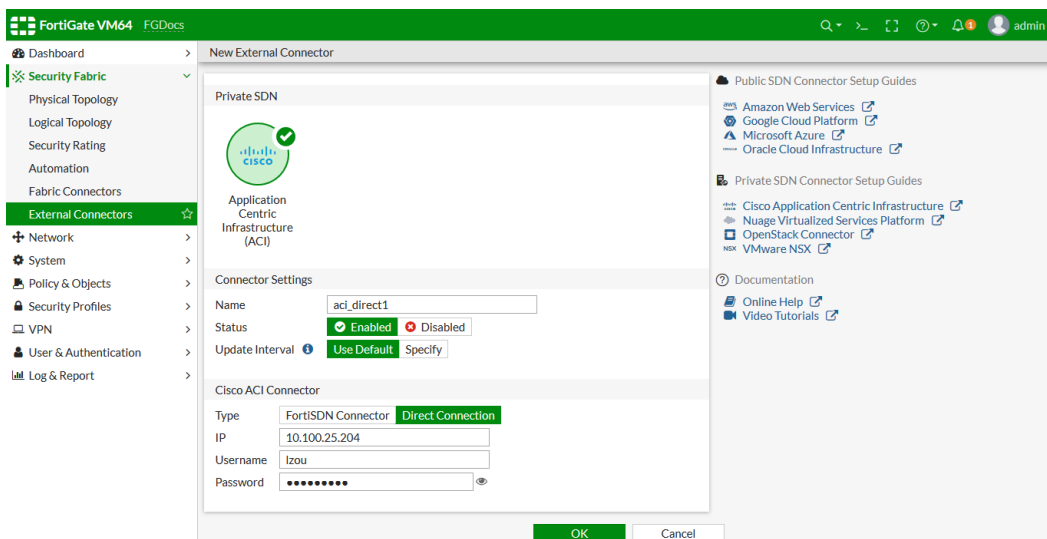
This connector supports the following address filters:

- Tenant
- Application
- Endpoint group
- Tag

### To configure a Cisco ACI connector in the GUI:

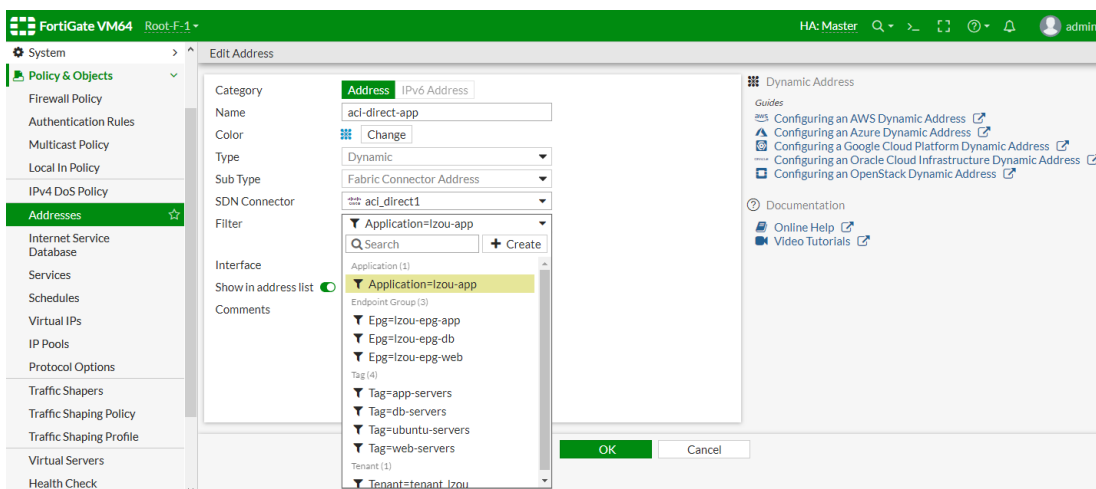
1. Create the Cisco ACI SDN connector:
  - a. Go to *Security Fabric > External Connectors* and click *Create New*.
  - b. In the *Private SDN* section, click *Application Centric Infrastructure (ACI)*.
  - c. Configure the *Connector Settings* as needed. The update interval is in seconds.
  - d. In the *Cisco ACI Connector* section, for *Type*, select *Direct Connection* and configure the remaining settings as needed.

e. Click OK.



2. Create a dynamic firewall address for the connector:

- a. Go to *Policy & Objects > Addresses*.
- b. Click *Create New > Address* and enter a name.
- c. Configure the following settings:
  - i. For *Type*, select *Dynamic*.
  - ii. For *Sub Type*, select *Fabric Connector Address*.
  - iii. For *SDN Connector*, select the connector created in step 1.
  - iv. For *Filter*, select an entry from the dropdown list. In this example, *Application* is selected.
- d. Click OK.





### 3. Confirm that the connector resolves the dynamic firewall IP addresses:

- Go to *Policy & Objects > Addresses*.
- In the address table, hover over the address created in step 2 to view which IP addresses it resolves to:

Name	Type	Details	Interface	Visibility	Ref.
aci-add-tag	Dynamic (ACI)			Visible	0
aci-direct-app	Dynamic (ACI-DIRECT)			Visible	0
aci-direct-end	Dynamic (ACI-DIRECT)			Visible	0
aci-direct-tag	Dynamic (ACI-DIRECT)			Visible	0
aci-direct-ten	Dynamic (ACI-DIRECT)			Visible	0
all-address-se	Dynamic (ALICLOUD)			Visible	0
all	Subnet	0.0.0.0/0		Visible	17
autoupdate.o	FQDN	autoupdate.opera.com		Visible	2
aws-address-tag-1	Dynamic (AWS)			Visible	0
aws-address-tag-2	Dynamic (AWS)			Visible	0
aws-address-wildcard	Dynamic (AWS)			Visible	0
aws-autoscale-1	Dynamic (AWS)			Visible	0
azure_add1	Dynamic (AZURE)			Visible	0
charlie_test	Dynamic (NSX)			Visible	0
csf_ns_group	Dynamic (NSX)			Visible	0
fgt	Dynamic (NSX)			Visible	0
gcp-address-node-1	Dynamic (GCP)			Visible	0
gcp-address-node-2	Dynamic (GCP)			Visible	0
gcp-address-wildcard	Dynamic (GCP)			Visible	0
gcp-ops	Dynamic (GCP)			Visible	0

### To configure a Cisco ACI connector in the CLI:

#### 1. Create the Cisco ACI SDN connector:

```
config system sdn-connector
  edit "aci_direct1"
    set status enable
    set type aci-direct
    set server "10.100.25.204"
    set username "lzou"
    set password xxxxxxxx
    set update-interval 60
  next
end
```

#### 2. Create a dynamic firewall address for the connector:

```
config firewall address
  edit "aci-direct-app"
    set type dynamic
    set sdn "aci_direct1"
    set color 17
    set filter "Application=lzou-app"
  next
end
```

#### 3. Confirm that the connector resolves the dynamic firewall IP addresses:

```
config firewall address
  edit "aci-direct-app"
    show
      config firewall address
        edit "aci-direct-app"
```

```

set uuid 794aaf20-3e33-51ea-57e1-10b5badf3fc7
set type dynamic
set sdn "aci_direct1"
set color 17
set filter "Application=lzou-app"
config list
  edit "10.0.5.11"
  next
  edit "10.0.5.12"
  next
  edit "10.0.6.11"
  next
  edit "10.0.6.12"
  next
  edit "10.0.6.13"
  next
  edit "10.0.6.14"
  next
  edit "10.0.7.11"
  next
  edit "10.0.7.12"
  next
end
next
end
next
end

```

## Configuring Cisco pxGrid SDN connector

You can create an endpoint connector to Cisco pxGrid by using FortiManager. FortiManager dynamically collects updates from pxGrid and forwards them to FortiGate by using the Fortinet Single Sign On (FSSO) protocol.

### To create a Cisco pxGrid SDN connector:

1. On FortiManager, create an SSO Connector to Cisco ISE.  
Communication between FortiManager and Cisco ISE is secured by using TLS. FortiManager requires a client certificate issued by Cisco ISE. FortiManager uses the certificate to authenticate to Cisco ISE.

The screenshot shows the 'Edit IPv4 Policy' configuration window in FortiManager. The left sidebar shows the 'Policy & Objects' tree with 'IPv4 Policy' selected. The main area contains the following fields:

- Name: (empty)
- Incoming Interface: any
- Outgoing Interface: any
- Source Internet Service: OFF
- Source Address: all
- Source User: (empty)
- Source User Group: ISE-group
- FSSO: ☒
- RSSO: ☐
- Destination Internet Service: OFF
- Destination Address: all
- Service: ALL
- Schedule: always
- Action: Deny, Accept, IPSEC (Accept is selected)
- Log Traffic: ☐ No Log, ☒ Log Security Events, ☐ Log All Sessions
- ☐ Generate Logs when Session Starts
- ☐ Capture Packets
- NAT: ☐
- Security Profiles: ☐
- Shared Shaper: (empty)
- Reverse Shaper: (empty)
- Per-IP Shaper: (empty)
- Comments: (empty)

At the bottom right, there are 'OK' and 'Cancel' buttons.

- On FortiManager, map Cisco ISE groups to a Fortinet FSSO group.  
Once a secured communication channel is established, Cisco sends all user groups to FortiManager. The FortiManager administrator can select specific groups and map them to Fortinet FSSO groups.

The screenshot shows the 'Edit User Group' configuration window in FortiManager. The left sidebar shows the 'Policy & Objects' tree with 'User Groups' selected. The main area contains the following fields:

- Group Name: ISE-group
- Type: ☐ Firewall, ☒ FSSO/Cisco TrustSec, ☐ GUEST, ☐ RADIUS Single Sign-On(RSSO)
- Members: (empty)

A 'Select Entries' dialog box is open, showing a list of entries. The entry 'px\_ise1\_Guests' is selected. The dialog box also shows a '1 Entry Selected' status and 'OK' and 'Cancel' buttons.

3. On FortiManager, add Fortinet FSSO group to a firewall policy in a policy package.

The screenshot shows the 'Edit IPv4 Policy' configuration page in FortiManager. The left sidebar shows the hierarchy: Policy Packages > Object Configurations > default > IPv4 Policy > Installation Targets. The main configuration area includes the following fields:

- Name: (empty)
- Incoming Interface: any
- Outgoing Interface: any
- Source Internet Service: OFF
- Source Address: all
- Source User: (empty)
- Source User Group: ISE-group
- FSSO: ☒
- RSSO: ☐
- Destination Internet Service: OFF
- Destination Address: all
- Service: ALL
- Schedule: always
- Action: Deny, Accept, IPSEC (Accept is selected)
- Log Traffic: ☐ No Log, ☒ Log Security Events, ☐ Log All Sessions
- Generate Logs when Session Starts: ☐
- Capture Packets: ☐
- NAT: ☐
- Security Profiles: ☐
- Shared Shaper: (empty)
- Reverse Shaper: (empty)
- Per-IP Shaper: (empty)
- Comments: (empty)

At the bottom right, there are 'OK' and 'Cancel' buttons.

4. On FortiManager, synchronize the policy package to the firewall for the managed FortiGate.

The screenshot shows the 'Install Wizard - Policy Package (default)' dialog box. The background shows the 'Device Manager' tab with a table of devices:

Device Name	Config Status	Policy Package Status	CU Template Status	Firmware Version
FortiGate-400D	Synchronized	default		FortiGate 6.2.0.build0866 (GA)

The dialog box shows the following progress:

- Installation Preparation Total: 2/2, Success: 2, Error: 0, Warning: 0
- Index 1: FortiGate-400D[copy] - root, Status: Copy to device done
- Index 2: Write summary[preview], Status: Write preview done
- Interface Validation: ☒
- Policy and Object Validation: ☒
- Ready to Install: ☒

At the bottom, there is a table with the following data:

Device Name	Status	Action
FortiGate-400D[root]	Connection Up	Install Preview, Policy Package Diff

At the bottom right, there are 'Install' and 'Cancel' buttons.

5. On FortiGate, verify that the synced firewall policy contains the correct FSSO group and that all FSSO-related information in user `adgrp` is correct.

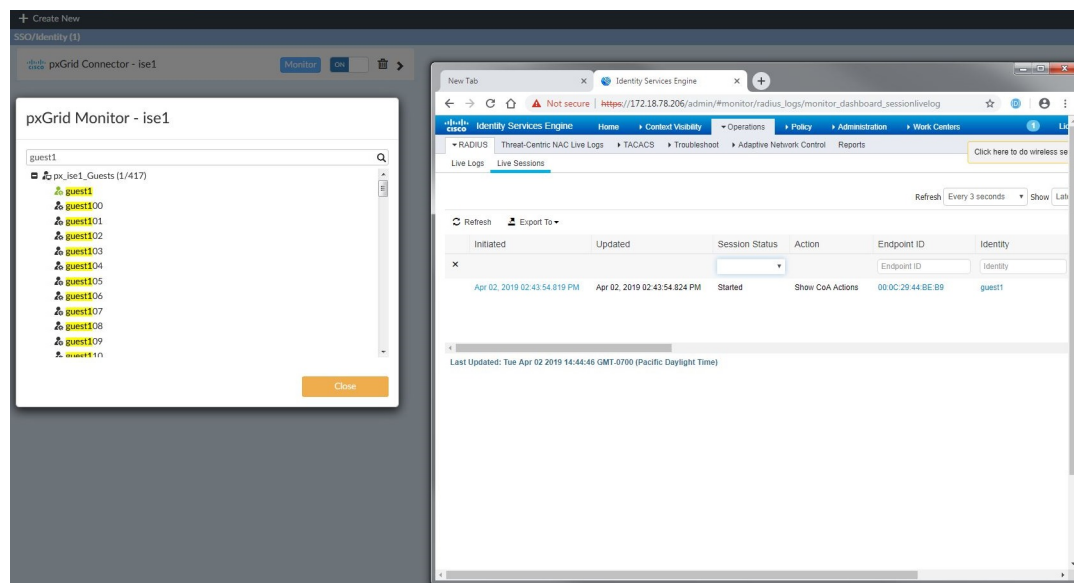
```

config firewall policy
edit 1
set uuid b803052e-562a-51e9-0561-82525c8bcaa9
set srcintf "any"
set dstintf "any"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set groups "ISE-group"
next
end

FortiGate-400D # show user adgrp
config user adgrp
edit "px_isel_ANY"
set server-name "FortiManager"
next
edit "px_isel_Agroup1"
set server-name "FortiManager"
next
edit "px_isel_Agroup2"
set server-name "FortiManager"
next
edit "px_isel_Auditors"
set server-name "FortiManager"
next
edit "px_isel_BYOD"
set server-name "FortiManager"
next
edit "px_isel_Contractors"
set server-name "FortiManager"
next
edit "px_isel_Developers"
set server-name "FortiManager"
next
edit "px_isel_Development_Servers"
set server-name "FortiManager"
next
edit "px_isel_Employees"
set server-name "FortiManager"
next
edit "px_isel_Guests"
set server-name "FortiManager"
next
edit "px_isel_HR"
set server-name "FortiManager"
next
edit "px_isel_Network_Services"
set server-name "FortiManager"

```

6. After successful user authentication on Cisco ISE, verify that information is forwarded to FortiManager. On FortiManager, the icon next to the authenticated user in *pxGrid Monitor* should be green.



FortiGate should have two entries: one in the firewall-authenticated user list and one in the FSSO logged-on user list.

In the FSSO logged-on user list, you can view both groups. You view the group that the user belongs to on Cisco ISE and the Fortinet FSSO group.

```

FortiGate-400D #
FortiGate-400D # dia deb authd fssso 1
-----FSSSO logons-----
IP: 10.1.100.188  User: guest1  Groups: px_isel_Guests  Workstation:  MemberOf: ISE-group
Total number of logons listed: 1, filtered: 0
-----end of FSSSO logons-----

FortiGate-400D # dia firewall auth 1
10.1.100.188, guest1
  type: fssso, id: 0, duration: 5969%, idled: 5969%
  server: FortiManager
  packets: in 0 out 0, bytes: in 0 out 0
  group_id: 2
  group_name: ISE-group

----- 1 listed, 0 filtered -----

```

## Multiple clusters on Cisco ACI connectors

You can include multiple ACI clusters used in availability for external Cisco ACI SDN connector VMs. When creating a Cisco ACI SDN connector, configuring multiple IPs allows the FortiGate to connect to SDN connector VMs in the same ACI cluster in a round-robin fashion. Only one SDN connector VM is active, and the remaining serve as backups if the active one fails. FortiOS 6.4.9 and later versions support this feature.

In this example, two Cisco ACI cluster SDN connectors are configured (*aci\_robot\_238* and *aci\_robot\_239*). Each cluster contains two Cisco ACI SDN connector VMs.

### To create ACI cluster SDN connectors in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. Select *Application Centric Infrastructure (ACI)* and configure the following:

<b>Name</b>	<i>aci_robot_238</i>
<b>Type</b>	Set to <i>FortiSDN Connector</i> .
<b>IP</b>	Enter two IP addresses: <i>10.6.30.38</i> and <i>10.6.30.238</i> .
<b>Port</b>	Set to <i>Specify</i> and enter <i>5671</i> .
<b>Username</b>	Enter the ACI username.
<b>Password</b>	Enter the ACI password.

**Edit External Connector**

**Private SDN**

Application Centric Infrastructure (ACI)

**Connector Settings**

Name: aci\_robot\_238

Status: Enabled Disabled

**Cisco ACI Connector**

Type: FortiSDN Connector Direct Connection

IP: 10.6.30.38

Port: Use Default Specify 5671

Username: admin

Password: Change

**Status**

Up

**Public SDN Connector Setup Guides**

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Oracle Cloud Infrastructure

**Private SDN Connector Setup Guides**

- Cisco Application Centric Infrastructure
- Nuage Virtualized Services Platform
- OpenStack Connector
- VMware NSX

**Documentation**

- Online Help
- Video Tutorials

**OK** **Cancel**

- Click **OK**.
- Repeat these steps to create another connector with the following settings:

<b>Name</b>	aci_robot_239
<b>Type</b>	Set to <i>FortiSDN Connector</i> .
<b>IP</b>	Enter two IP addresses: 10.6.30.39 and 10.6.30.239.
<b>Port</b>	Set to <i>Specify</i> and enter 5671.
<b>Username</b>	Enter the ACI username.
<b>Password</b>	Enter the ACI password.

#### To create dynamic addresses associated with the connectors in the GUI:

- Go to *Policy & Objects > Addresses* and click *Create New > Address*.
- Configure the following:

<b>Name</b>	aci-add-App-238
<b>Type</b>	Dynamic
<b>Sub Type</b>	Fabric Connector Address
<b>SDN Connector</b>	aci_robot_238
<b>Tenant</b>	Fortinet
<b>Endpoint Group Name</b>	App1

- Click **OK**.
- Repeat these steps to create another dynamic address with the following settings:

<b>Name</b>	<i>aci-add-App-239</i>
<b>Type</b>	<i>Dynamic</i>
<b>Sub Type</b>	<i>Fabric Connector Address</i>
<b>SDN Connector</b>	<i>aci_robot_239</i>
<b>Tenant</b>	<i>Fortinet</i>
<b>Endpoint Group Name</b>	<i>App1</i>

To test that firewall addresses can resolve the dynamic addresses based on the SDN connector in the GUI:

- Go to **Policy & Objects > Addresses**.
- Hover the cursor over an address. The tooltip shows the resolved addresses of the dynamic firewall address.

Name	Details	Interface	Fabric Sync	Type	Ref.
aci-add-App-238	aci-add-App-238		Disable	Address	0
aci-add-App-239	aci-add-App-239		Disable	Address	0

Address: aci-add-App-239

Type: Dynamic

Sub Type: Fabric Connector Address

SDN Connector: aci\_robot\_239

Tenant: Fortinet

Endpoint Group Name: App1

Interface: any

Resolved To:

57.244.141.1	42.204.249.3	113.20.146.15
222.20.244.24	136.111.120.28	232.68.132.53
159.10.165.63	158.68.111.87	193.182.254.90
153.11.53.97	137.225.232.98	127.139.171.102
246.238.232.107	189.130.189.117	145.225.9.121
61.85.89.127	254.63.148.141	255.101.230.147
164.95.140.151	118.223.37.174	213.112.26.175
67.82.175.177	171.90.109.180	15.216.40.190
106.97.0.201	247.186.79.208	112.237.77.209
21.90.161.213	156.8.243.247	79.85.64.251

Fabric Sync: Disabled

References: 0



**To create ACI cluster SDN connectors in the CLI:**

```

config system sdn-connector
  edit "aci_robot_238"
    set type aci
    set server-list "10.6.30.38" "10.6.30.238"
    set server-port 5671
    set username "admin"
    set password *****
  next
  edit "aci_robot_239"
    set type aci
    set server-list "10.6.30.39" "10.6.30.239"
    set server-port 5671
    set username "admin"
    set password *****
  next
end

```

**To create dynamic addresses associated with the connectors in the CLI:**

```

config firewall address
  edit "aci-add-App-238"
    set type dynamic
    set sdn "aci_robot_238"
    set color 17
    set tenant "Fortinet"
    set epg-name "App1"
  next
  edit "aci-add-App-239"
    set type dynamic
    set sdn "aci_robot_239"
    set color 17
    set tenant "Fortinet"
    set epg-name "App1"
  next
end

```

**To test that firewall addresses can resolve the dynamic addresses based on the SDN connector in the CLI:****1. Check the aci-add-App-238 address:**

```

# diagnose firewall dynamic address aci-add-App-238
aci_robot_238.aci.Fortinet.App1.*: ID(90)
  ADDR(244.141.232.3)
  ADDR(124.37.216.5)
  ADDR(178.77.227.6)
  ...
  ADDR(87.26.255.252)
  ADDR(31.45.199.254)
  ADDR(154.149.224.254)

Total dynamic list entries: 1.
Total dynamic addresses: 150
Total dynamic ranges: 0

```

**2. Check the aci-add-App-239 address:**

```
# diagnose firewall dynamic address aci-add-App-239
aci_robot_239.aci.Fortinet.Appl.*: ID(91)
  ADDR(57.244.141.1)
  ADDR(42.204.249.3)
  ADDR(113.20.146.15)
  ...
  ADDR(21.90.161.213)
  ADDR(156.8.243.247)
  ADDR(79.85.64.251)

Total dynamic list entries: 1.
Total dynamic addresses: 30
Total dynamic ranges: 0
```

# Change log

Date	Change description
2020-08-05	Initial release.
2020-08-20	Updated <a href="#">Configuring the Cisco ACI connector in FortiOS on page 17.</a>
2020-08-21	Updated <a href="#">SDN Connector integration with Cisco ACI on page 17.</a> Added <a href="#">Configuring VDOM and SDN connector example on page 17.</a>
2020-09-22	Updated <a href="#">Configuring the Cisco ACI connector in FortiOS on page 17.</a>
2021-02-18	Added <a href="#">Configuring Cisco pxGrid SDN connector on page 58.</a>
2021-11-02	Added <a href="#">HA on Cisco ACI using FGCP over FGSP on page 4.</a>
2022-04-26	Added <a href="#">Multiple clusters on Cisco ACI connectors on page 62.</a>
2024-03-06	Updated <a href="#">Configuring FortiOS on page 12.</a>



**FORTINET®**



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.