FortiOS - Fortinet Device Package 2.3 for Cisco ACI

Version 6.0.3

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
https://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

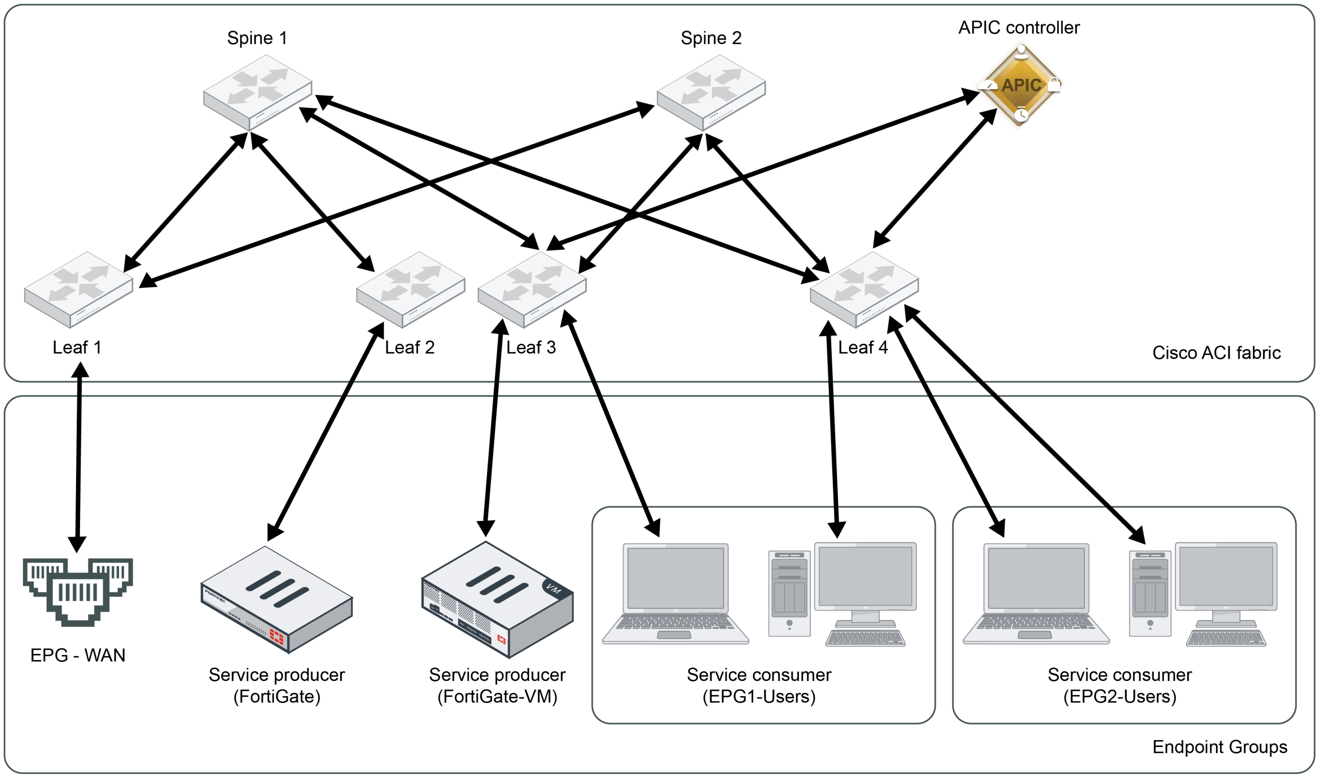
March 26, 2019
FortiOS 6.0.3 Fortinet Device Package 2.3 for Cisco ACI
01-603-548098-20190326

TABLE OF CONTENTS

Overview

Fortinet Device Package for Cisco Application Centric Infrastructure (ACI), previously called FortiGate for Cisco ACI, is the Fortinet solution for providing seamless integration between FortiGate/FortiManager firewall deployments with Cisco Application Policy Infrastructure Controller (APIC). This integration allows customers to perform single point of FortiGate/FortiManager configuration and management operation through the Cisco APIC. This device package breaks down into Service Manager Mode (FortiManager) and Service Policy Mode (FortiGate).

While the FortiGate series of firewalls enables superb firewall services, the insertion, configuration, and management of network services such as a firewall can be complex and error-prone tasks in a data center environment. One solution for such data center problems is Cisco ACI. Cisco ACI is a policy-based framework with integration of software and hardware in the underlying leaf-spine fabric. In Cisco ACI, the APIC is a tool used to automate service insertion and provisioning into the fabric of the network environment. Network service appliances, both physical and virtual, can be attached to the ACI fabric's leaf node through APIC. Traffic demanding certain network services is steered by APIC-managed policies to the appropriate resources. The Fortinet Device Package allows FortiGate to be included amongst the list of resources that traffic can be directed to.



Licensing

Fortinet Device Package for Cisco ACI is available free of charge for Fortinet customers. You must ensure that you register your FortiGate/FortiManager with FortiCare on Fortinet Customer Service & Support.

Supported new features

Fortinet Device Package for Cisco ACI 2.3 supports the following functions:

- Service Manager mode. See Deploying Service Manager Mode on page 9.
- VLAN trunking for virtual FortiGate. See Configuring VLAN Trunking for FortiGate-VM on page 15.
- Multiple services per policy rule. See Adding multiple services per policy rule on page 16.

Supported Fortinet products

Supported Fortinet products refer to those that are compatible with the Fortinet Device Package for Cisco ACI software, and will properly integrate into the Cisco ACI. To support Fortinet Device Package for Cisco ACI, you must have one of the listed FortiGate models running one of the supported firmware versions.

Models

Fortinet Device Package for Cisco ACI 2.3 supports integration with the following predefined models:

- FortiGate-300D
- FortiGate-600D
- FortiGate-800D
- FortiGate-900D
- FortiGate-1000C
- FortiGate-1000D
- FortiGate-1200D
- FortiGate-1500D
- FortiGate-3000D
- FortiGate-3100D
- FortiGate-3200D
- FortiGate-3700D
- FortiGate-3980E
- FortiGate-6300
- FortiGate-6500
- FortiGate-VM

Firmware

Fortinet Device Package for Cisco ACI 2.3 is compatible with FortiOS 6.0.3.

Prerequisites

The following prerequisites must be met before deploying Fortinet Device Package for Cisco ACI:

- Cisco-side prerequisites on page 7
- FortiGate-side prerquisites on page 7
- FortiManager-side prerequisites on page 8

Cisco-side prerequisites

Before Fortinet Device Package for Cisco ACI can be successfully deployed, a number of prerequisites must be satisfied within the Cisco environment. A Cisco ACI 3.2 or later environment must be in place. Within Cisco, the following configurations must be completed before the Fortinet Device Package can be deployed:

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

For details, consult the Cisco APIC deployment guide.

Any pre-existing L4-L7 configuration based on the Fortinet Device Package 1.3 or 2.x must be reconfigured.

FortiGate-side prerquisites

Before Fortinet Device Package for Cisco ACI can be successfully deployed, a number of prerequisites must be satisfied on the FortiGate:

Physical Firewall

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.

VM firewall

1. Assign the network ports before starting the VM.
2. Configure the administrator username and password.
3. Enable HTTP/HTTPS on the management port.
4. Configure the management port's IP address.
5. Enable VDOM-Admin globally.

FortiManager-side prerequisites

Before the Fortinet Device Package can be successfully deployed, 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(s) with FortiManager.

Fortinet Service Manager Mode

Service Manager Mode is an additional solution to the Cisco ACI platform provided by Fortinet Technologies Inc.. This new device package automates the configuration push from Cisco ACI to FortiManager. The type of configuration generated through the Cisco ACI relates to network components only. The user must configure the service policy in FortiManager.

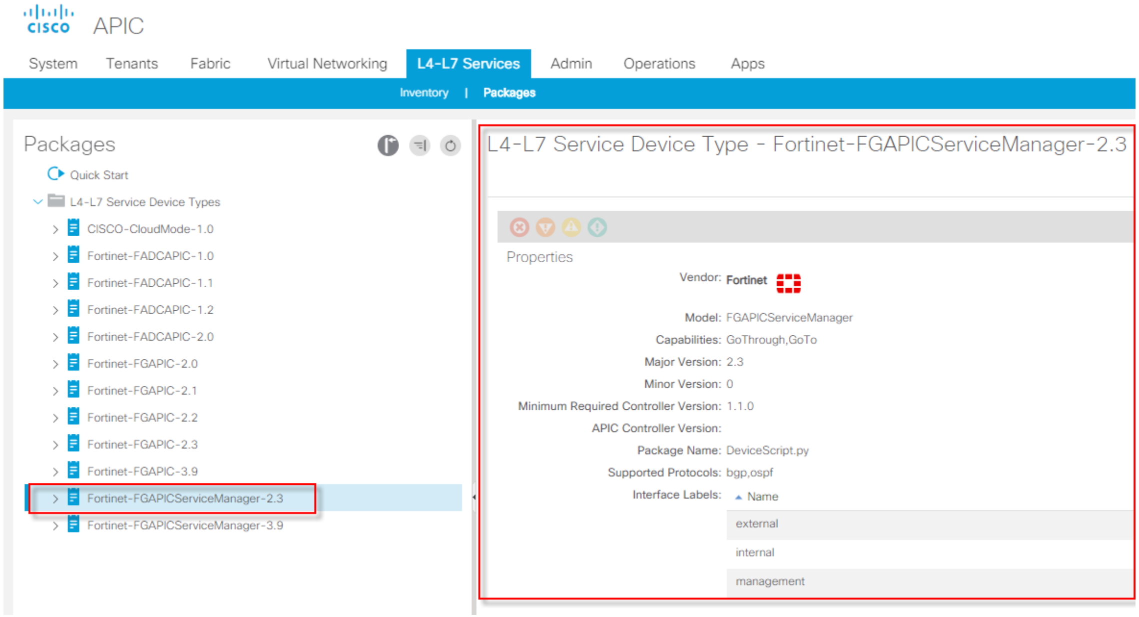
Deploying Service Manager Mode

The below sections provide a walk-through of deploying a service insertion within Service Manager Mode:

1. Import Fortinet Device Package into Cisco ACI.
2. Define the device manager.
3. Define L4-L7 devices and map to the defined device manager.
4. Define the functional profile.
5. Create the service graph template.
6. Deploy the service graph to FortiManager.
7. Ensure that the service graph is deployed.

To import Fortinet Device Package into Cisco ACI:

1. In Cisco APIC, go to *L4-L7 Services* > *Packages*.
2. Import the Fortinet-FGAPICServiceManager-2.3 as shown.



L4-L7 Service Device Type - Fortinet-FGAPICServiceManager-2.3

Properties

Vendor: Fortinet

Model: FGAPICServiceManager

Capabilities: GoThrough,GoTo

Major Version: 2.3

Minor Version: 0

Minimum Required Controller Version: 1.1.0

APIC Controller Version:

Package Name: DeviceScript.py

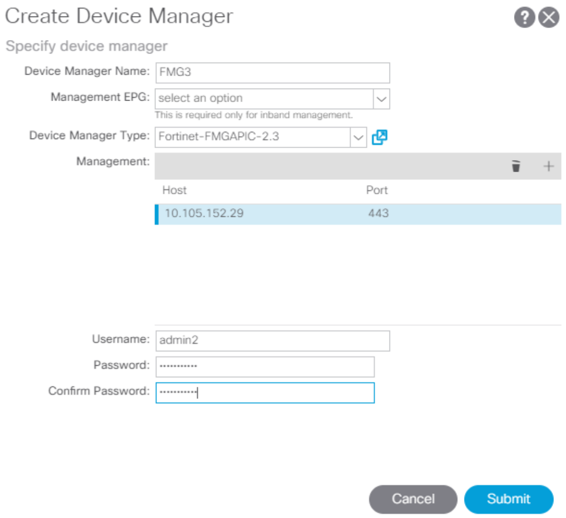
Supported Protocols: bgp,ospf

Interface Labels:

Name
external
internal
management

To define device managers:

1. Go to *Tenant* > *L4-L7* > *Services* > *Device Manager*.
2. Right-click, then select *Create Device Manager*.
3. In the *Management* field, enter the FortiManager IP address.
4. In the *Username* and *Password* fields, provide the FortiManager login information. Click *Submit*.



Create Device Manager

Specify device manager

Device Manager Name: FMG3

Management EPG: select an option

This is required only for inband management.

Device Manager Type: Fortinet-FMGAPIC-2.3

Management:

Host	Port
10.105.152.29	443

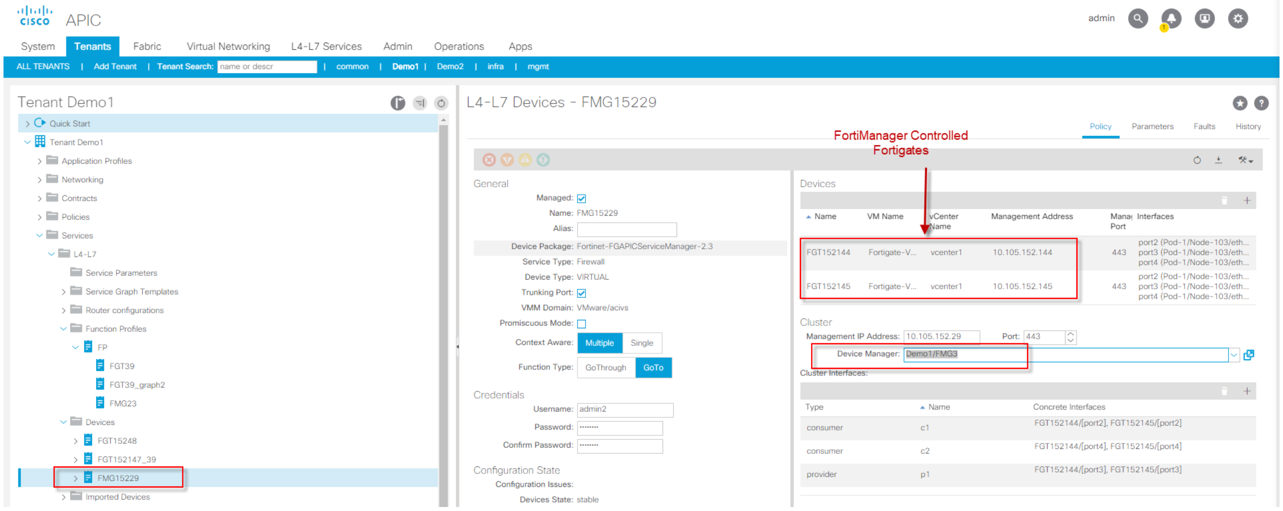
Username: admin2

Password: ••••••••••

Confirm Password: ••••••••••

To define L4-L7 devices and map to the defined device manager:

1. Go to *Tenant* > *L4-L7* > *Devices*.
2. Define all FortiGates controlled by the FortiManager.
3. For all L4-L7 devices, map to the FortiManager in the *Device Manager* field.



L4-L7 Devices - FMG15229

General

Managed: ☑

Name: FMG15229

Alias:

Device Package: Fortinet-FGAPICServiceManager-2.3

Service Type: Firewall

Device Type: VIRTUAL

Trunking Port: ☑

VMM Domain: VMware/acivs

Promiscuous Mode: □

Context Aware: Multiple | Single

Function Type: GoThrough | GoTo

Credentials

Username: admin2

Password: ••••••••

Confirm Password: ••••••••

Configuration State

Configuration Issues:

Devices State: stable

Devices

Name	VM Name	vCenter Name	Management Address	Mana; Port	Interfaces
FGT152144	Fortigate-V...	vcenter1	10.105.152.144	443	port2 (Pod-1/Node-103/eth... port3 (Pod-1/Node-103/eth... port4 (Pod-1/Node-103/eth...
FGT152145	Fortigate-V...	vcenter1	10.105.152.145	443	port2 (Pod-1/Node-103/eth... port3 (Pod-1/Node-103/eth... port4 (Pod-1/Node-103/eth...

Cluster

Management IP Address: 10.105.152.29 Port: 443

Device Manager: Demo1/FMG3

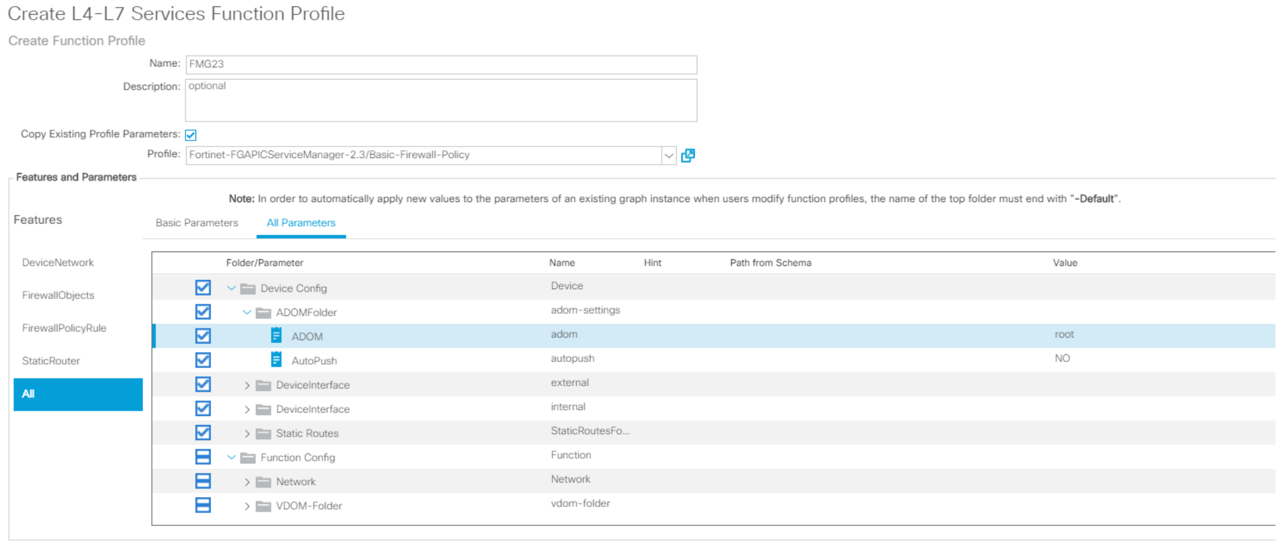
Cluster Interfaces:

Type	Name	Concrete Interfaces
consumer	c1	FGT152144/[port2], FGT152145/[port2]
consumer	c2	FGT152144/[port4], FGT152145/[port4]
provider	p1	FGT152144/[port3], FGT152145/[port3]

To define the functional profile:

1. Go to *Tenant* > *Services* > *L4-L7* > *Functional Profiles*.
2. Right-click, then select *Create L4-L7 Services Function Profile*.

3. Create a functional profile as shown.



Create L4-L7 Services Function Profile

Create Function Profile

Name: FMG23

Description: optional

Copy Existing Profile Parameters: ☑

Profile: Fortinet-FGAPICServiceManager-2.3/Basic-Firewall-Policy

Features and Parameters

Note: In order to automatically apply new values to the parameters of an existing graph instance when users modify function profiles, the name of the top folder must end with "**-Default**".

Features: DeviceNetwork, FirewallObjects, FirewallPolicyRule, StaticRouter, All

Basic Parameters | All Parameters

	Folder/Parameter	Name	Hint	Path from Schema	Value
☑	Device Config	Device			
☑	ADOMFolder	adom-settings			
☑	ADOM	adom			root
☑	AutoPush	autopush			NO
☑	DeviceInterface	external			
☑	DeviceInterface	internal			
☑	Static Routes	StaticRoutesFo...			
⊟	Function Config	Function			
⊟	Network	Network			
⊟	VDOM-Folder	vdom-folder			

4. Enable the *ADOMFolder* folder. The folder contains the following parameters:

Parameter	Description
ADOM	Enter the name of the ADOM to deploy the VDOM to. If the ADOM does not exist, the VDOM is programmed to be deployed to the ADOM that the FortiGate is residing on. For example, if you enter ADOM1 for this parameter and ADOM1 exists on the FortiManager, the VDOM is created under ADOM1. However, if ADOM1 does not exist on the FortiManager and the FortiGate is controlled by the root ADOM, the VDOM is created under the root ADOM.
AutoPush	Choose whether to push the configuration to the FortiGate(s) after the VDOM is created within FortiManager. Note that the configuration is serially pushed to the FortiGate list defined under L4-L7 devices. If you have configured the settings to use zones in conjunction with AutoPush, the zone information does not appear on the FortiGate(s) until the policy is pushed to them.

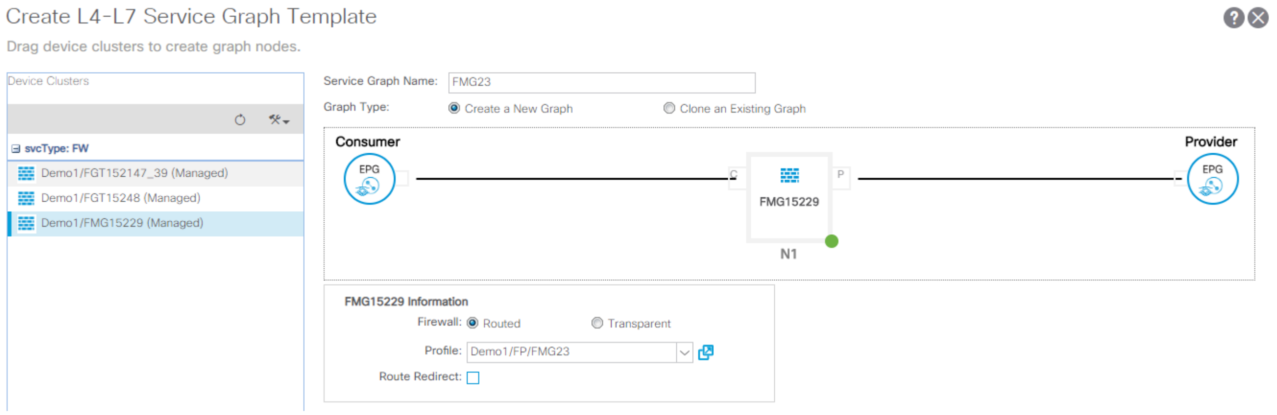
The *VDOM-Folder* folder also contains an *AdomSettings* parameter. Ignore this parameter as it is just a placeholder.

5. For all L4-L7 devices, map to the FortiManager in the *Device Manager* field.

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.



Create L4-L7 Service Graph Template

Drag device clusters to create graph nodes.

Device Clusters

svcType: FW
- Demo1/FGT152147_39 (Managed)
- Demo1/FGT15248 (Managed)
- Demo1/FMG15229 (Managed)

Service Graph Name: FMG23

Graph Type: ● Create a New Graph ○ Clone an Existing Graph

FMG15229 Information

Firewall: ● Routed ○ Transparent

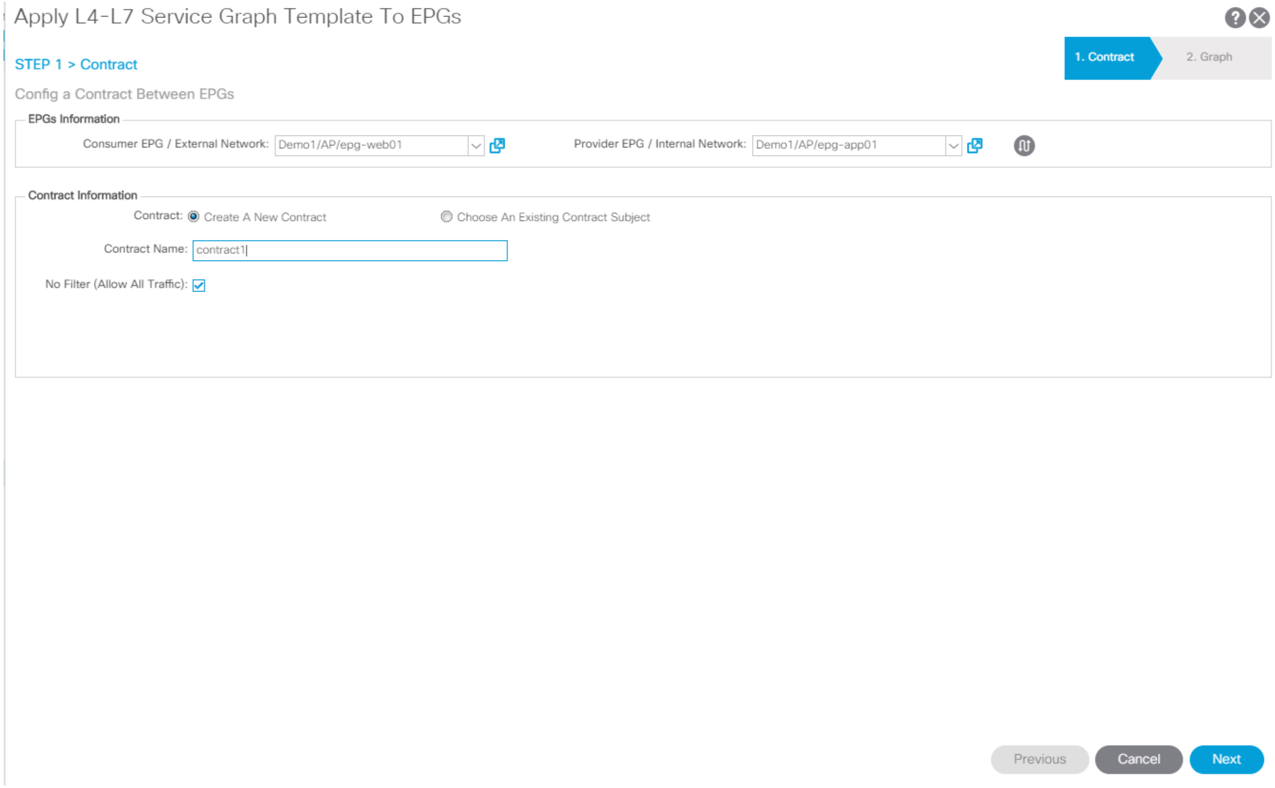
Profile: Demo1/FP/FMG23

Route Redirect: □

3. Click *Submit*.

To deploy the service graph to FortiManager:

1. Go to *Tenant* > *Services* > *L4-L7* > *Service Graph Templates*. Right-click the newly created service graph template, then select *Apply L4-L7 Service Graph Template*.
2. Configure the desired EPGs for the *Consumer EPG / External Network* and *Provider EPG / Internal Network* dropdown lists.
3. Enter a contract name.
4. Click *Next*.



Apply L4-L7 Service Graph Template To EPGs

STEP 1 > Contract

Config a Contract Between EPGs

EPGs Information

Consumer EPG / External Network: Demo1/AP/epg-web01

Provider EPG / Internal Network: Demo1/AP/epg-app01

Contract Information

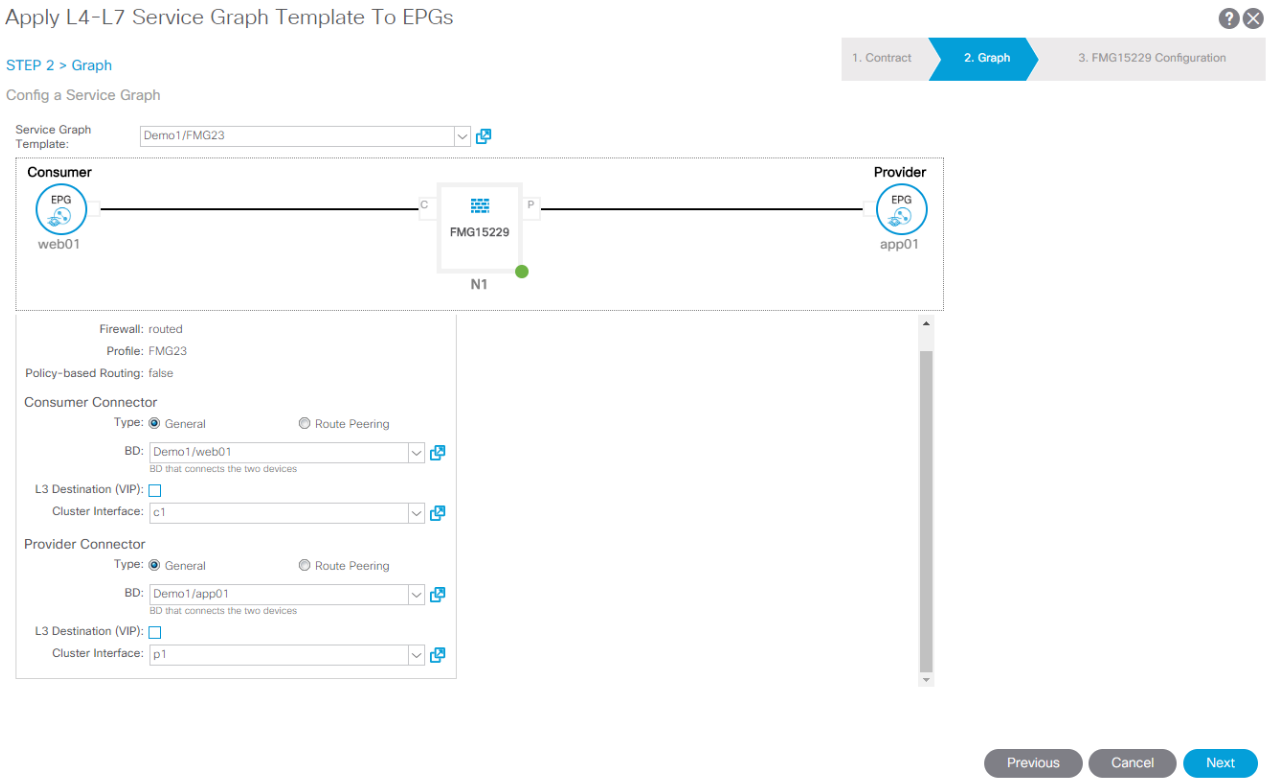
Contract: ● Create A New Contract ○ Choose An Existing Contract Subject

Contract Name: contract1

No Filter (Allow All Traffic): ☑

5. From the *Service Graph Template* dropdown list, select the service graph template configured earlier.
6. Configure the consumer and provider connectors.

7. Click *Next*.



Apply L4-L7 Service Graph Template To EPGs

STEP 2 > Graph

Config a Service Graph

Service Graph Template: Demo1/FMG23

Firewall: routed

Profile: FMG23

Policy-based Routing: false

Consumer Connector

Type: ● General ○ Route Peering

BD: Demo1/web01

BD that connects the two devices

L3 Destination (VIP): □

Cluster Interface: c1

Provider Connector

Type: ● General ○ Route Peering

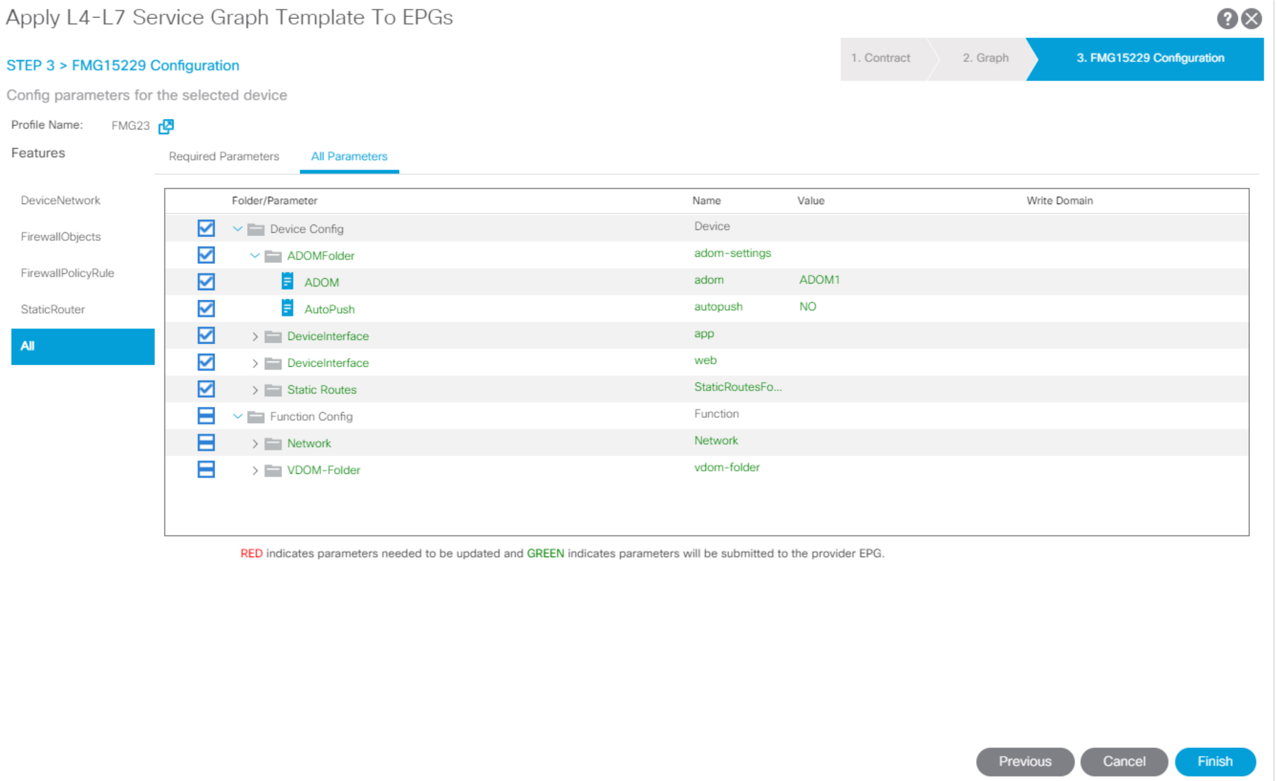
BD: Demo1/app01

BD that connects the two devices

L3 Destination (VIP): □

Cluster Interface: p1

8. Select the desired parameters for the device. Click *Finish*. The service graph is deployed.



Apply L4-L7 Service Graph Template To EPGs

STEP 3 > FMG15229 Configuration

Config parameters for the selected device

Profile Name: FMG23

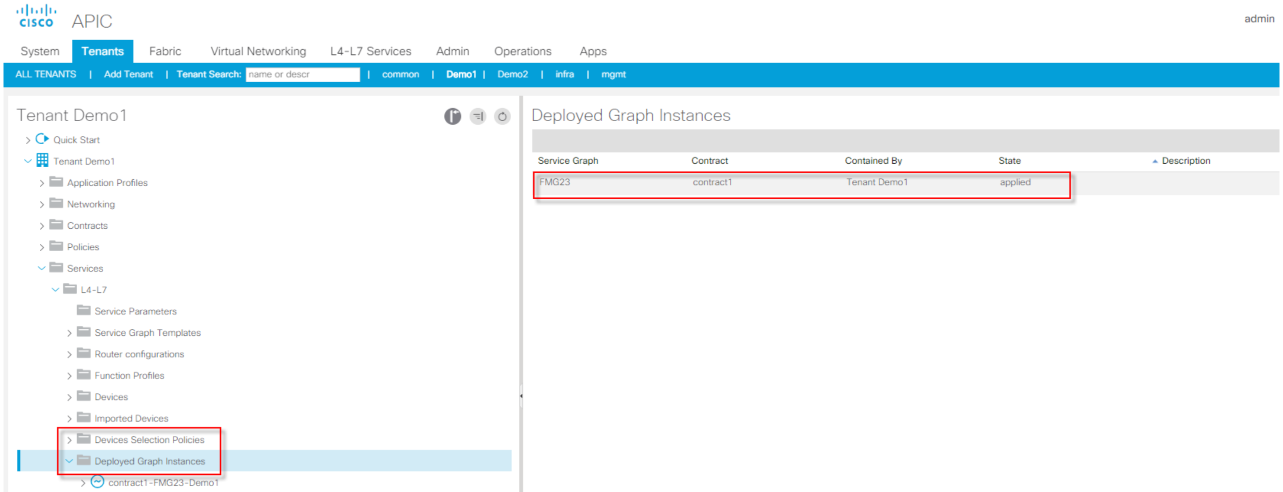
Features

	Folder/Parameter	Name	Value	Write Domain
☑	Device Config	Device		
☑	ADOMFolder	adom-settings		
☑	ADOM	adom	ADOM1	
☑	AutoPush	autopush	NO	
☑	DeviceInterface	app		
☑	DeviceInterface	web		
☑	Static Routes	StaticRoutesFo...		
⊟	Function Config	Function		
⊟	Network	Network		
⊟	VDOM-Folder	vdom-folder		

RED indicates parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

To ensure that the service graph is deployed:

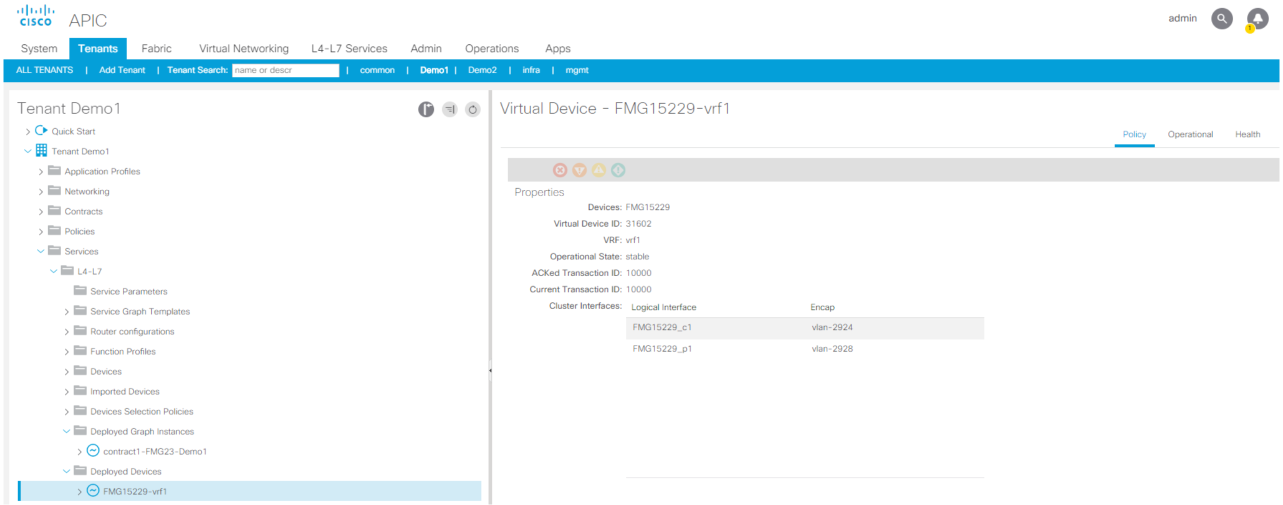
1. Go to *Tenant* > *Services* > *L4-L7* > *Deployed Graph Instances*. Ensure that the service graph has been deployed.



Deployed Graph Instances

Service Graph	Contract	Contained By	State	Description
FMG23	contract1	Tenant Demo1	applied	

2. Go to *Tenant* > *Services* > *L4-L7* > *Deployed Devices*.



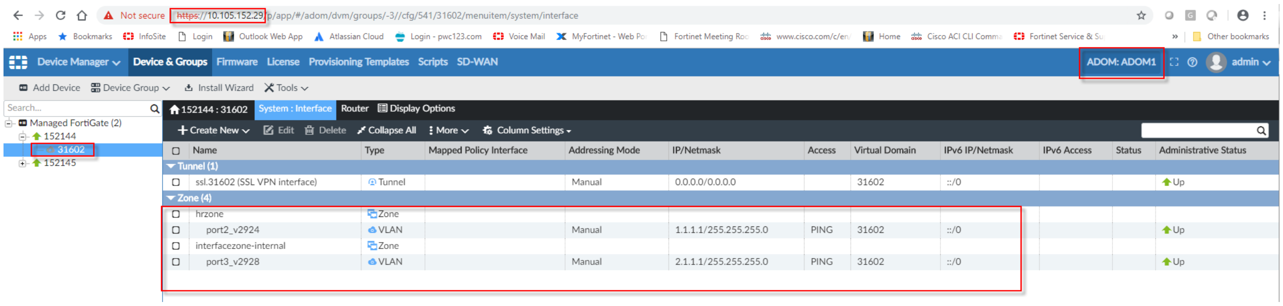
Virtual Device - FMG15229-vrf1

Properties

Devices: FMG15229
Virtual Device ID: 31602
VRF: vrf1
Operational State: stable
ACKed Transaction ID: 10000
Current Transaction ID: 10000
Cluster Interfaces:

Logical Interface	Encap
FMG15229_c1	vlan-2924
FMG15229_p1	vlan-2928

3. In FortiManager, ensure that deployment was successful.



	Name	Type	Mapped Policy Interface	Addressing Mode	IP/Netmask	Access	Virtual Domain	IPv6 IP/Netmask	IPv6 Access	Status	Administrative Status
	Tunnel (1)										
□	ssl.31602 (SSL VPN interface)	Tunnel		Manual	0.0.0.0/0.0.0.0		31602	::/0			Up
	Zone (4)										
□	hrzone	Zone									
□	port2_v2924	VLAN		Manual	1.1.1.1/255.255.255.0	PING	31602	::/0			Up
□	interfacezone-internal	Zone									
□	port3_v2928	VLAN		Manual	2.1.1.1/255.255.255.0	PING	31602	::/0			Up

Configuring VLAN Trunking for FortiGate-VM

FortiGate-VM now supports VLAN trunking, similar to physical FortiGate implementation. When this feature is enabled, a VLAN interface is created on the FortiGate-VM instead of a physical port.

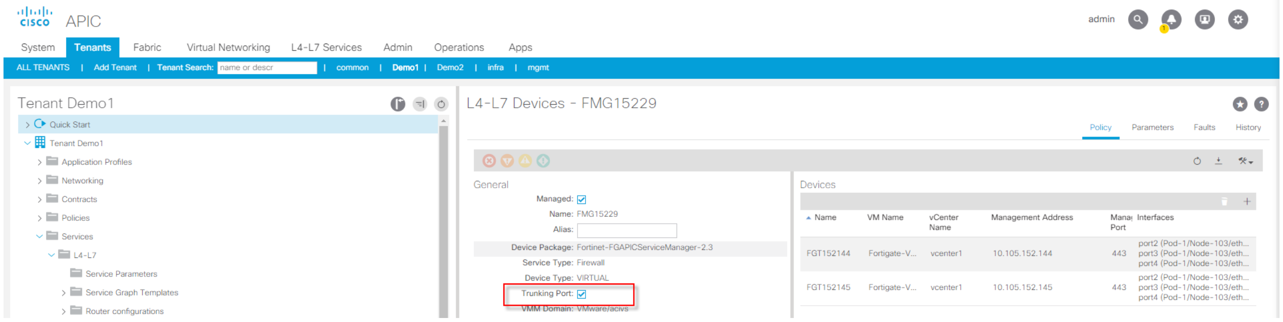
1. Configure the trunk port group.
2. Configure the L4-L7 device to use the trunk.
3. Deploy the service graph template.

To configure the trunk port group:

1. In Cisco APIC, go to *Virtual Networking* > *VMM Domains* > *VMware* > *vcentername* > *Trunk Port Groups*.
2. Configure the following:
   a. Specify the VLAN ranges. By default, the VLAN list is taken from the domain's VLAN namespace.
   b. Specify the trunk port group immediacy. By default, this is on-demand.
   c. Enable or disable promiscuous mode. By default, this is disabled.
   d. Enable or disable MAC changes. By default, this is enabled.
   e. Enable or disable forged transmits. By default, this is enabled.

To configure the L4-L7 device to use the trunk:

1. Go to *Tenant* > *Services* > *L4-L7* > *Devices* > *devicename*.
2. Select the *Trunking Port* checkbox.



L4-L7 Devices - FMG15229

General

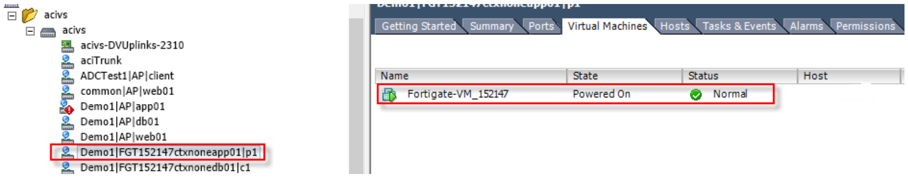
Managed: ☑
Name: FMG15229
Alias:
Device Package: Fortinet-FGAPICServiceManager-2.3
Service Type: Firewall
Device Type: VIRTUAL
Trunking Port: ☑
VMM Domain: VMware/acivs

Devices

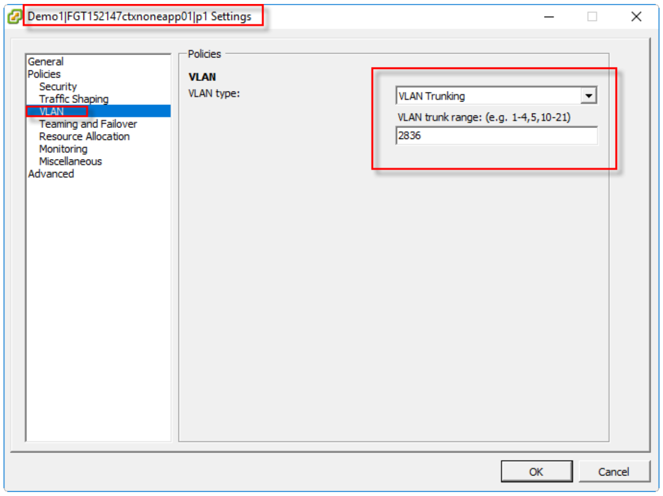
Name	VM Name	vCenter Name	Management Address	Mana Port	Interfaces
FGT152144	Fortigate-V...	vcenter1	10.105.152.144	443	port2 (Pod-1/Node-103/eth... port3 (Pod-1/Node-103/eth... port4 (Pod-1/Node-103/eth...
FGT152145	Fortigate-V...	vcenter1	10.105.152.145	443	port2 (Pod-1/Node-103/eth... port3 (Pod-1/Node-103/eth... port4 (Pod-1/Node-103/eth...

To modify ACI dvSwitch's portgroup to trunking:

In vCenter, modify the ACI dvSwitch to place VNICs into trunk port groups and set the VLAN type to VLAN Trunking.



Name	State	Status	Host
Fortigate-VM_152147	Powered On	Normal	



Demo1|FGT152147ctxnoneapp01|p1 Settings

Policies

VLAN

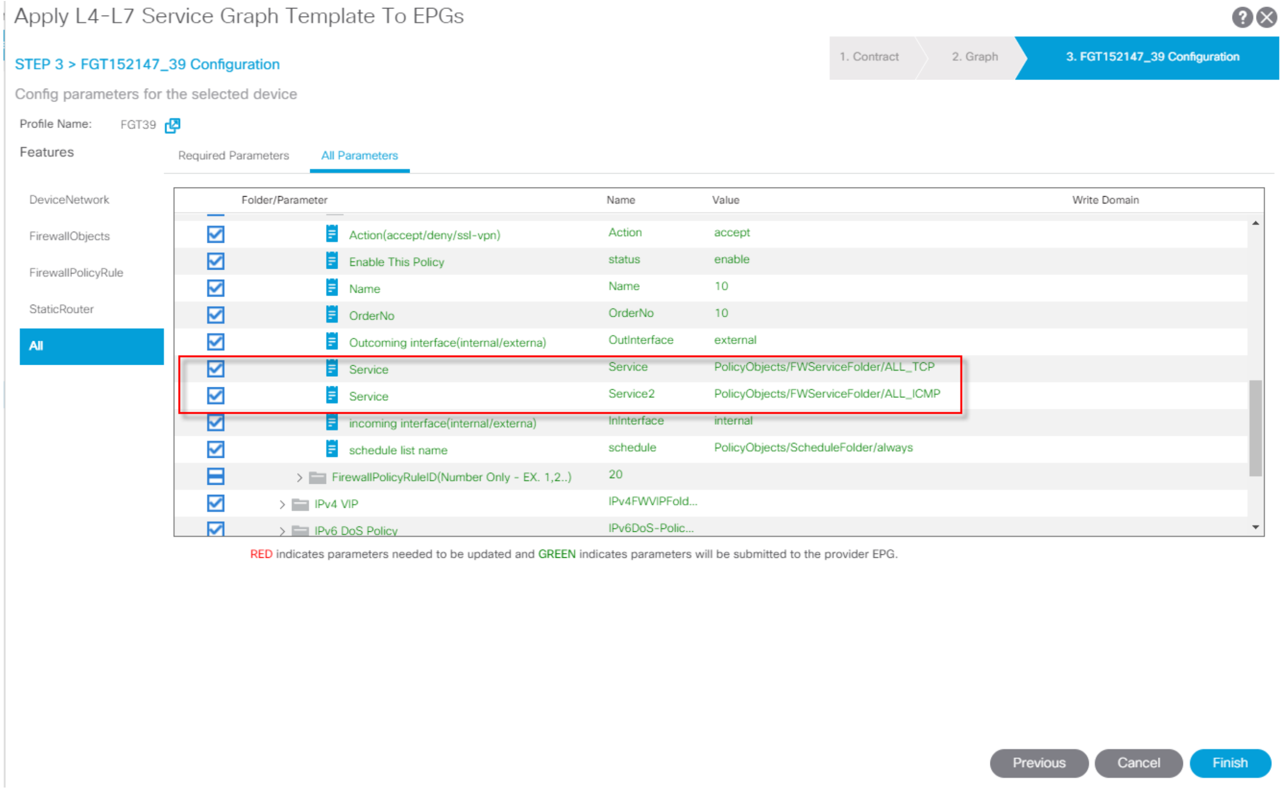
VLAN type: VLAN Trunking

VLAN trunk range: (e.g. 1-4,5,10-21)

2836

Adding multiple services per policy rule

You can add multiple services within a single policy rule. The example shows a policy rule with multiple services as configured in Cisco APIC, which is then deployed to the FortiGate.



Apply L4-L7 Service Graph Template To EPGs

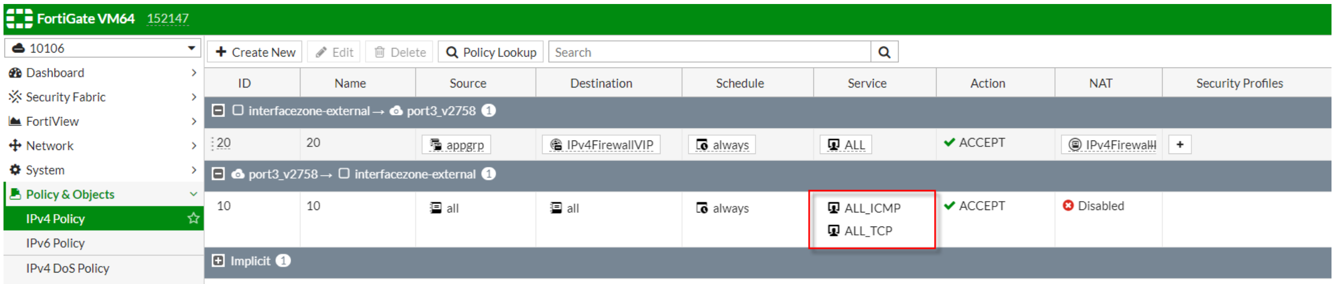
STEP 3 > FGT152147_39 Configuration

Config parameters for the selected device

Profile Name: FGT39

	Folder/Parameter	Name	Value	Write Domain
☑	Action(accept/deny/ssl-vpn)	Action	accept	
☑	Enable This Policy	status	enable	
☑	Name	Name	10	
☑	OrderNo	OrderNo	10	
☑	Outcoming interface(internal/externa)	OutInterface	external	
☑	Service	Service	PolicyObjects/FWServiceFolder/ALL_TCP	
☑	Service	Service2	PolicyObjects/FWServiceFolder/ALL_ICMP	
☑	incoming interface(internal/externa)	InInterface	internal	
☑	schedule list name	schedule	PolicyObjects/ScheduleFolder/always	
⊟	> FirewallPolicyRuleID(Number Only - EX. 1,2..)	20		
☑	> IPv4 VIP	IPv4FWVIPFold...		
☑	> IPv6 DoS Policy	IPv6DoS-Polic...		

RED indicates parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
interfacezone-external → port3_v2758 1								
20	20	appgrp	IPv4FirewallVIP	always	ALL	✓ ACCEPT	IPv4Firewall	+
port3_v2758 → interfacezone-external 1								
10	10	all	all	always	ALL_ICMP ALL_TCP	✓ ACCEPT	✗ Disabled	
Implicit 1								

Change log

Date	Change Description
2019-03-26	Initial release.