



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

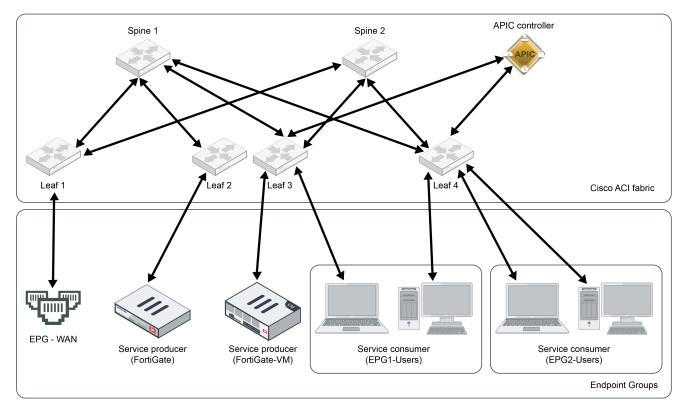
TABLE OF CONTENTS

| Overview | 4 |
|---|----|
| Licensing | 5 |
| Supported new features | 5 |
| Supported Fortinet products | 5 |
| Models | 5 |
| Firmware | |
| Prerequisites | 7 |
| Cisco-side prerequisites | 7 |
| FortiGate-side prerquisites | 7 |
| Physical Firewall | 7 |
| VM firewall | 8 |
| FortiManager-side prerequisites | 8 |
| Fortinet Service Manager Mode | 9 |
| Deploying Service Manager Mode | 9 |
| Configuring VLAN Trunking for FortiGate-VM1 | 15 |
| Adding multiple services per policy rule1 | 16 |
| Change log1 | 8 |

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.

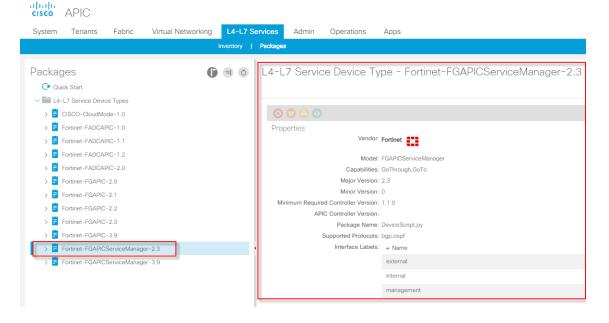
Deploying Service Manager Mode

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.



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 N | Manager | | ? ⊗ |
|----------------------|--|--------|------------|
| Specify device manag | er | | |
| Device Manager Name: | FMG3 | | |
| Management EPG: | select an option This is required only for inband manag | ement. | |
| Device Manager Type: | Fortinet-FMGAPIC-2.3 | ~ 🛃 | |
| Management: | | | ¥ + |
| | Host | Port | |
| | 10.105.152.29 | 443 | |
| | | | |
| | | | |
| | | | |
| Username: | admin2 | | |
| Password: | | | |
| Confirm Password: | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Cancel | Submit |

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.

| L TENANTS Add Tenant Tenant Search: name or descr | common Demo1 Demo | ttions Apps | | |
|---|-----------------------|---|--|---|
| | | c 1 mile 1 million | | |
| enant Demo1 | 0 🗉 🛈 | L4-L7 Devices - FMG15229 | | 6 |
| > O Quick Start | × | | | Policy Parameters Faults H |
| - 🧱 Tenant Demo1 | | | FortiManager Controlled | |
| > Application Profiles | | | Fortigates | 0 ± • |
| > III Networking | | General | Devices | |
| > E Contracts | | Managed: 🗹 | 001100 | |
| > Policies | | Name: FMG15229 | Name VM Name vCenter Managemen | |
| V Services | | Alias: | Name | Port |
| ✓ □ L4-L7 | | Device Package: Fortinet-FGAPICServiceManager-2.3 | FGT152144 Fortigate-V vcenter1 10.105.152. | .144 port2 (Pod-1/Node-103/etl 443 port3 (Pod-1/Node-103/etl |
| Service Parameters | | Service Type: Firewall Device Type: VIRTUAL | | port4 (Pod-1/Node-103/eth port2 (Pod-1/Node-103/eth |
| > Service Graph Templates | | Trunking Port: | FGT152145 Fortigate-V vcenter1 10.105.152 | .145 443 port3 (Pod-1/Node-103/eth |
| > Router configurations | | VMM Domain: VMware/acivs | 4 | port4 (Pod-1/Node-103/eth |
| V Function Profiles | | Promiscuous Mode: | Cluster | |
| ✓ ■ FP | | Context Aware: Multiple Single | Management IP Address: 10.105.152.29 Port: 443 | v |
| FGT39 | | Function Type: GoThrough GoTo | Device Manager: Demo1/FMG3 | ~ |
| FGT39_graph2 | | Controligit Control | Cluster Interfaces: | |
| FMG23 | | Credentials | | |
| V Devices | | Username: admin2 | | Concrete Interfaces FGT152144/[port2], FGT152145/[port2] |
| > FGT15248 | | Password: | consumer ci | |
| y 🔤 (0110240 | | Confirm Password: | consumer c2 | FGT152144/[port4], FGT152145/[port4] |

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 Se | ervices Function Profile | | |
|-----------------------------|--|---|--|
| Create Function Profile | | | |
| | Name: FMG23 | | |
| Desc | ription: optional | | |
| Copy Existing Profile Parar | neters: 🗹 | | |
| | Profile: Fortinet-FGAPICServiceManager-2.3/Basic-Firewa | all-Policy 🗸 🔁 | |
| Features and Parameters | | | |
| Features | Note: In order to automatically apply new of Basic Parameters All Parameters | values to the parameters of an existing graph instance when users modify function profiles, | the name of the top folder must end with "-Default". |
| DeviceNetwork | Folder/Parameter | Name Hint Path from Schema | Value |
| FirewallObjects | 🗹 🗸 🔚 Device Config | Device | |
| | Market ADOMFolder | adom-settings | |
| FirewallPolicyRule | ADOM | adom | root |
| StaticRouter | AutoPush | autopush | NO |
| All | > 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 Gra | ph Template | |
|--------------------------------------|---|----------|
| Drag device clusters to create graph | nodes. | |
| Device Clusters | Service Graph Name: FMG23 | |
| Ó | Graph Type: Create a New Graph Clone an Existing Graph | |
| svcType: FW | Consumer | Provider |
| Demo1/FGT152147_39 (Managed) | C P | EPG |
| Demo1/FGT15248 (Managed) | FMG15229 | |
| Demo1/FMG15229 (Managed) | | |
| | N1 | |
| | | |
| | 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.

| 1 > Contract | | | | 1. Contract 2. Graph |
|---|---------------|---|------------|----------------------|
| | | | | |
| a Contract Between EPGs | | | | |
| Information | | | | |
| Consumer EPG / External Network: Demo1/AP/epg-web | 01 🗸 🕑 | Provider EPG / Internal Network: Demo1/AP/epg-app01 | - P | |
| ract Information | | | | |
| Contract: Create A New Contract | Choose An Exi | isting Contract Subject | | |
| Contract Name: contract1 | | | | |
| o Filter (Allow All Traffic): 🗸 | , | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | Previo | us Cancel Nex |

- 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.

8.

| the a Service Graph | | | EPGs | | 1 Contract | |
|---|--|---|---------------------------|--|----------------|---------------------------------|
| <pre>data prefer to read of the set of the device. Click Finish. The service graph is deployed. prefer to read of the set of the device. Click Finish. The service graph is deployed. prefer to read of the set of the device. Click Finish. The service graph is deployed. prefer to read of the set of the device. Click Finish. The service graph is deployed. prefer to read of the set of the device. Click Finish. The service graph is deployed. prefer to read of the set of the device. Click Finish. The service graph is deployed. prefer to read of the set of the device. Click Finish. The service graph is deployed. prefer to read of the set of the device. Click Finish. The service graph is deployed. prefer to read of the set of the device. Click Finish and the set of the device. Click finish and the set of the device. Click finish and the set of the device of the devic</pre> | P 2 > Graph | | | | 1. Contract 2. | Graph 3. FMG15229 Contiguration |
| <pre>part vertice vert</pre> | fig a Service Grap | h | | | | |
| Control Provider Provider <th>rvice Graph</th> <th>emo1/FMG23</th> <th>~ 🗗</th> <th></th> <th></th> <th></th> | rvice Graph | emo1/FMG23 | ~ 🗗 | | | |
| Image: Second | | | | | Provider | |
| Image: State of the second devices Image: State o | \frown | | | | \frown | |
| web31 | | | | | | |
| Firewelt : rund Profile: : PAG23 Site: - based Roung: file: | web01 | | FMG15229 | | app01 | |
| Firewelt : rund Profile: : PAG23 Site: - based Roung: file: | | | | | | |
| Purdle: MO3 step-based bodies Sing-based bodies <td></td> <td></td> <td>N1</td> <td></td> <td></td> <td></td> | | | N1 | | | |
| <pre>sty-based Bouting: falls parameters for the selected devices. ty Deter interface:</pre> | Firewall: r | outed | | | - | |
| ansigner Connector | Profile: F | MG23 | | | | |
| Type: @ not a Version iii do contention (VP): | olicy-based Routing: fa | alse | | | | |
| B: Devolution | | | | | | |
| Is Destination (Willy Connector Type: © Connector | | | | | | |
| 13 Decision (VPP) <pre> Custor interface: i i</pre> | | | ~ 🗳 | | | |
| Outset interface: ovider Connector B0: Destination (Mipp)1 B1: Destination (Mipp)1 B2: Destination (Mipp)1 | | | | | | |
| Type: © Route Peering B) Destination (VP); Cancel N ect the desired parameters for the device. Click Finish. The service graph is deployed. b) L4-L7 Service Graph Template To EPGs P3 > FMG15229 Configuration P3 > FMG15229 Configuration P3 > FMG15229 Configuration Norme Value Virtual 0. Graph F000 Contract Norme Value Wite Domain Worklowski P1 > Endering Parameters (A) Parameters P3 > FMG15229 Contract 0. Contract (2. Graph) 1. Contract (2. Graph) (2. Graph)< | | | ~ 🖉 | | | |
| BD: Centrol / app01 BD: Deminol / app | ovider Connector | | | | | |
| Bit Bit is to water in the two dealers Boestination (With Endealers) Cluster Interface Previous Cancel No Section (Section (Sec | Type: (| General © Route Peering | | | | |
| L3 Destination (VIP): Custer Interface: pt = | BD: | Demo1/app01 | ~ 🖉 | | | |
| Cluster Interface 1 Cluste | | | | | | |
| Previous Cancel ect the desired parameters for the device. Click Finish. The service graph is deployed. ply L4-L7 Service Graph Template To EPGs P 3 - FMG15229 Configuration fg parameters for the selected device. fg parameters for the selected device. te Name Voce Worketwork evallObjects worketwork Image: Config | | | | | | |
| ect the desired parameters for the device. Click Finish. The service graph is deployed. ply L4-L7 Service Graph Template To EPGs P 3 > FMG15229 Configuration fig parameters for the selected device le Name: FMG2 C Required Parameters AI Parameters viceNetwork ViceNetwork | Guster Interrace: | b. | | | | |
| FMd23 Required Parameters Al Parameters viceNetwork Folder/Parameter Name Value Write Domain viceNetwork Folder/Parameter Device Device ViceNamin viceNetwork Folder/Parameter Device Device ViceNamin viceNetwork Folder/Parameter Device Device ViceNamin viceNetwork Folder/Parameter adom ADOM1 ViceNamin viceNetwork AltoPush adom ADOM1 ViceNamin viceNetwork AutoPush autopush No ViceNamin viceNetwork Name About ViceNamin ViceNamin viceNetwork AutoPush adom About ViceNamin viceNetwork MiceNetwork MiceNetwork | Gluster Internace: | μ 1 | | | v | |
| Required Parameters All Parameters viceNetwork Folder/Parameter Name Value Write Domain evallObjects Image: Config Device Device Device evallObjects Image: Config adom - settings DoM - Config Device evallObjects Image: Config adom - settings Device Device image: Config adom - settings adom - settings Device Device Image: Config adom - settings adom - settings Device Device Image: Config adom - settings adom - settings Device Device Device Image: Config adom - settings adom - settings Adom - settings Device Device Image: Config adom - settings adom - settings adom - settings Device Device Device Device De | ect the des | ired parameters for the ervice Graph Template To I | e device. Click <i>Fi</i> | <i>nish</i> . The service gra | | |
| viceNetWork Folder/Parameter Folder/Parameter Config Device Config Device Config Confi | ect the des ply L4-L7 Se P 3 > FMG15229 (| ired parameters for the ervice Graph Template To I Configuration | e device. Click <i>Fi</i> | nish. The service gra | | |
| ewallObjects | ect the des ply L4-L7 Se P 3 > FMG15229 (fig parameters for | Fired parameters for the ervice Graph Template To I Configuration the selected device | e device. Click <i>Fi</i> | nish. The service gra | | |
| evallObjects | ect the des ply L4-L7 Se P 3 > FMG15229 (fig parameters for le Name: FMG23 | sired parameters for the ervice Graph Template To I Configuration the selected device ♂ | e device. Click <i>Fi</i> | <i>nish</i> . The service gra | | |
| Image: State Routes adom-settings ewallPolicyRule Image: State Routes ticRouter Image: State Routes Image: State Routes State Routes Image: State Routes State Routes Image: State Routes State Routes | ect the des ply L4-L7 Se fig parameters for le Name: FMG23 tures | eired parameters for the ervice Graph Template To I Configuration the selected device Prequired Parameters All Parameters | e device. Click <i>Fi</i> | | 1. Contract 2. | 3rsph 3. FMG15229 Configuration |
| ewallPolicyRule Image: ADOM adom ADOM1 ticRouter Image: AutoPush autopush NO Image: Image | ect the des ply L4-L7 Se ply L4-L7 Se ply L4-L7 Se ply L4-L7 Se ply L4-L7 ply L4-L7 se ply L4-L4 | ervice Graph Template To I configuration the selected device Required Parameters All Parameters Folder/Parameter | e device. Click <i>Fi</i> | Name Valu | 1. Contract 2. | 3rsph 3. FMG15229 Configuration |
| Image: Second and and a second a secon | ect the des ply L4-L7 Se ply L4-L7 Se ply L4-L7 Se ply L4-L7 Se ply L4-L7 ply L4-L7 se ply L4-L4 | bired parameters for the ervice Graph Template To I Configuration the selected device Required Parameters All Parameters Folder/Parameter Folder/Parameter | e device. Click <i>Fi</i> | Name Valu Device | 1. Contract 2. | 3rsph 3. FMG15229 Configuration |
| Image: Constraint of the constr | ect the des ply L4-L7 Se P 3 > FMG15229 (fig parameters for le Name: FMG23 tures viceNetwork ewallObjects | bired parameters for the ervice Graph Template To I Configuration the selected device Required Parameters All Parameters Folder/Parameter Folder/Parameter | e device. Click <i>Fi</i> | Name Valu Device adom-settings | 1. Contract 2. | 3rsph 3. FMG15229 Configuration |
| Image: Constraint of the second se | ect the des ply L4-L7 Se P 3 > FMG15229 (fig parameters for le Name: FMG23 tures viceNetwork ewallObjects ewallPolicyRule | sired parameters for the ervice Graph Template To I Configuration the selected device Image: Required Parameters All Parameters Folder/Parameter Image: Polycler Config Image: Polycler Config <td>e device. Click <i>Fi</i></td> <td>Name Valu Device adom-settings adom AD</td> <td>1. Contract 2.</td> <td>3rsph 3. FMG15229 Configuration</td> | e device. Click <i>Fi</i> | Name Valu Device adom-settings adom AD | 1. Contract 2. | 3rsph 3. FMG15229 Configuration |
| Image: Static Routes Static RoutesFo Image: Static Courtes Fo Function Config | ect the des ply L4-L7 Se P 3 > FMG15229 (fig parameters for le Name: FMG23 tures viceNetwork ewallObjects ewallObjects ewallObjects ewallObjects | sired parameters for the ervice Graph Template To I Configuration the selected device Image: Required Parameters All Parameters Folder/Parameter Image: Polyce Config | e device. Click <i>Fi</i> | Name Valu Device adom-settings adom AD autopush NO | 1. Contract 2. | 3rsph 3. FMG15229 Configuration |
| Function Config Function | ect the des ply L4-L7 Se P 3 > FMG15229 (fig parameters for le Name: FMG23 tures viceNetwork ewallObjects ewallObjects ewallObjects ewallObjects | bired parameters for the ervice Graph Template To I Configuration the selected device | e device. Click <i>Fi</i> | Name Valu Device adorm-settings adorm ADi autopush NO app | 1. Contract 2. | 3rsph 3. FMG15229 Configuration |
| | ect the des ply L4-L7 Se P 3 > FMG15229 (fig parameters for le Name: FMG23 tures viceNetwork ewallObjects ewallObjects ewallObjects | Formulation the selected device Image: Parameters All Parameters Folder/Parameter Image: Polycology Polycology AutoPush Image: Polycology Image: Poly | e device. Click <i>Fi</i> | Name Valu Device adom-settings adom ADi autopush NO app web | 1. Contract 2. | 3rsph 3. FMG15229 Configuration |
| | ect the des ply L4-L7 Se P 3 > FMG15229 (fig parameters for le Name: FMG23 tures viceNetwork ewallObjects ewallObjects ewallObjects | Ford parameters for the envice Graph Template To I configuration the selected device Image: Configure Parameters All Parameters Folder/Parameter Image: Configure Parameters Folder/Parameter Image: Configure Parameters Folder/Parameter Image: Configure Parameter Image: Configure Parameter < | e device. Click <i>Fi</i> | Name Valu Device adom-settings adom ADi autopush NO app web StaticRoutesFo | 1. Contract 2. | 3rsph 3. FMG15229 Configuration |

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

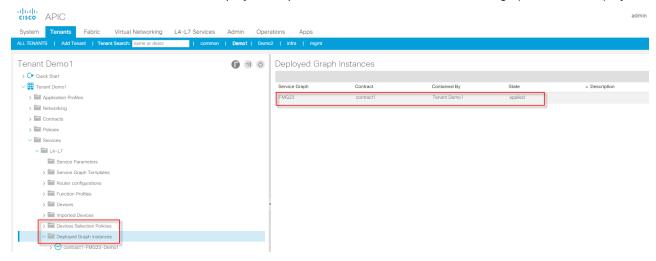
vdom-folder

> VDOM-Folder

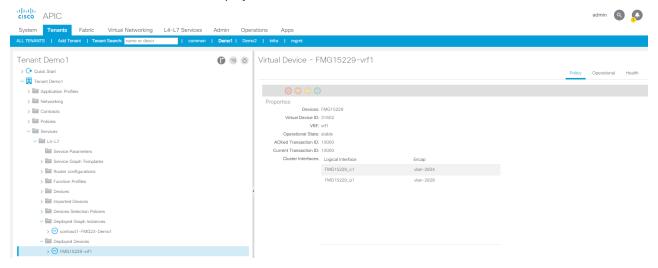
Previous Cancel Finish

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.



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



3. In FortiManager, ensure that deployment was successful.

| | ecure https://10.105.152.29 p/app/#/adom/dvm nfoSite 🗋 Login 🚺 Outlook Web App 🗼 Atlas: | | | | 🗅 Fortinet Meeting Roo 📸 www | w.cisco.com/c/e | n/ 🔛 Home 📸 (| Cisco ACI CLI Comma 🔃 | Fortinet Service & Su | | Image: Image: Ima |
|---------------------------------------|--|----------------------------|----------------------------|------------------|------------------------------|-----------------|----------------|------------------------|-----------------------|----------|--|
| Device Manager 🗸 D | zvice & Groups Firmware License Provision | ing Templates | Scripts SD-WAN | | | | | | AD | OM: ADOM | 1 🖸 🛛 🖉 🚺 admin |
| 🗖 Add Device 🖀 Device Gr | oup 🗸 👌 Install Wizard 🗙 Tools 🗸 | | | | | | | | _ | | _ |
| arch | Q 152144:31602 System:Interface R | outer 🖽 Displa | y Options | | | | | | | | |
| ■ Managed FortiGate (2) → 152144 | + Create New 🗸 🖻 Edit 📋 Delete | 💉 Collapse All | 🗄 More 🗸 🛛 🙃 Column Settin | igs - | | | | | | | |
| - 🛋 31602 | Name | Туре | Mapped Policy Interface | Addressing Mode | IP/Netmask | Access | Virtual Domain | IPv6 IP/Netmask | IPv6 Access | Status | Administrative Status |
| + 152145 | 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 | | | | | | | | | |
| | | 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.

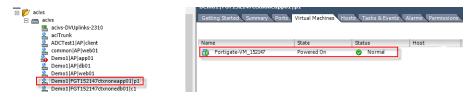
To configure the L4-L7 device to use the trunk:

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

| cisco APIC | | | | | | | admin | 0 |) 🖸 | ٢ |
|--|------------|---|--------------------------|-------------|-----------------|--------------------|-------------|------------------------|--|------------------|
| System Tenants Fabric Virtual Networkin ALL TENANTS Add Tenant Tenant Search: name or des | | | | | | | | | | |
| Tenant Demo1 | () | L4-L7 Devices - FMG15229 | | | | | | | | O |
| > 💽 Quick Start | <u>^</u> | | | | | | Policy | Parameters | Faults | Histo |
| V 🧱 Tenant Demo1 | | | | | | | | | | |
| > Application Profiles | | | | | | | | | 0 3 | <u>*</u> *. |
| > 📰 Networking | | General | Devices | | | | | | | |
| > Contracts | | Managed: 🗹 | | | | | | | | ÷ + |
| > Policies | | Name: FMG15229 Alias: | Name | VM Name | vCenter Name | Management Address | Man Port | al Interfaces | | |
| ~ 🖬 L4-L7 | | Device Package: Fortinet-FGAPICServiceManager-2.3 Service Type: Firewall | FGT152144 | Fortigate-V | vcenter1 | 10.105.152.144 | 443 | port3 (Po | d-1/Node-1 d-1/Node-1 d-1/Node-1 | 03/eth |
| Service Parameters Service Graph Templates | | Device Type: VIRTUAL Trunking Port: 🗹 | FGT152145 | Fortigate-V | vcenter1 | 10.105.152.145 | 443 | port2 (Po port3 (Po | d-1/Node-1 | 03/eth 03/eth |
| > 📰 Router configurations | | VMM Domain: VMware/acivs | | | | | | | | |

To modify ACI dvSwitch's portgroup to trunking:

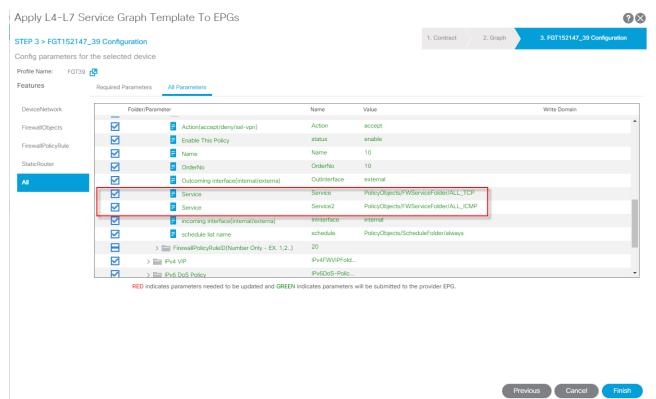
In vCenter, modify the ACI dvSwitch to place VNICs into trunk port groups and set the VLAN type to VLAN Trunking.



| Demo1 FGT152147ctxnonea | pp01 p1 Settings | | - | | × |
|--|--------------------------------|--|-----------------|-----|------|
| General Policies Security Traffic Shaping VAAN Teaming and Falover Resource Allocation Monitoring Miscelaneous Advanced | Policies VLAN VLAN type: | VLAN Trunking VLAN trunk range: (e. 2836 | g. 1-4,5,10-21) | • | |
| 1 | | | ОК | Car | ncel |

Adding multiple services per policy rule

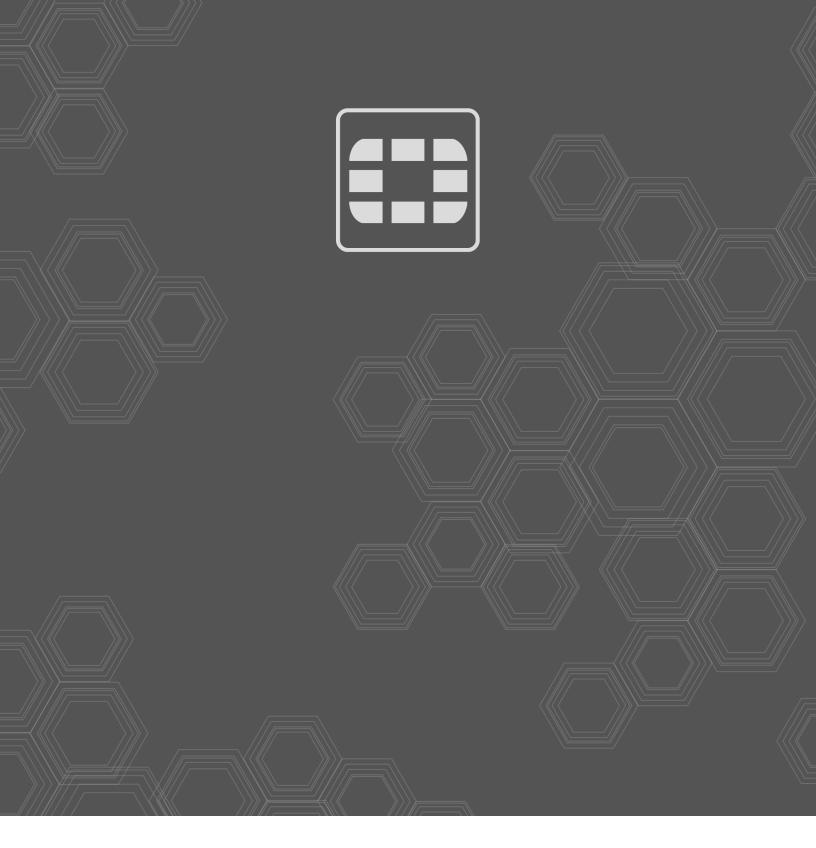
You can add multiple services within a single policy rule. The example shows a policy rule with multiple services as configured in Cisco APIC, which is then deployed to the FortiGate.



| d 10106 | • | + Create New | 🖋 Edit 📋 Dele | te Q Policy Lookup | Search | | Q | | | |
|-----------------------------|---|--------------|--|---------------------------|-----------------|-----------|----------|----------|-------------|-------------------|
| B Dashboard | > | ID | Name | Source | Destination | Schedule | Service | Action | NAT | Security Profiles |
| Security Fabric ■ FortiView | > | Interfacez | cone-external \rightarrow \bigcirc p | ort3_v2758 1 | | | | | | |
| Network | > | 20 | 20 | appgrp | IPv4FirewallVIP | always | I ALL | ✓ ACCEPT | IPv4Firewa₩ | + |
| System | > | of port3_v27 | $758 \rightarrow \Box$ interfacezo | ne-external 1 | | | | | | |
| Policy & Objects | ~ | 10 | 10 | 🔳 all | 🗉 all | o always | ALL ICMP | ✓ ACCEPT | Disabled | |
| IPv4 Policy | ☆ | 10 | 10 | an an | all all | LO always | | • ACCELL | Disabica | |
| IPv6 Policy | | | | | | | ALL_TCP | | | |
| IPv4 DoS Policy | | 🗄 Implicit 1 | | | | | | | | |

Change log

| Date | Change Description |
|------------|--------------------|
| 2019-03-26 | Initial release. |
| | |
| | |
| | |





Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiGare® 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 performances 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.