FortiGate Connector for Cisco ACI - Deployment Package

Version 6.0.1
# TABLE OF CONTENTS

**About FortiGate Connector for Cisco ACI** .......................................................... 6  
  Recommended minimum resources ................................................................. 6  
  Licensing ............................................................................................................ 7  
  Supported Fortinet products ........................................................................... 8  
    Firmware versions .......................................................................................... 8  
    Models .......................................................................................................... 8  
  Terms and concepts .......................................................................................... 10  
    Application network profiles ....................................................................... 10  
    Bridge domain (BD) ..................................................................................... 10  
    Contract ....................................................................................................... 10  
    End point group (EPG) ............................................................................... 10  
    FortiGate VDOMs ......................................................................................... 10  
  FortiOS RESTful API ........................................................................................ 10  
    North-south and east-west traffic ................................................................. 11  
    Tenant ......................................................................................................... 11  
    Virtual router and forwarding (VRF) ......................................................... 11  
  Special notice ................................................................................................... 11  
    Service manager mode: AutoPush feature interact with zoning ............... 11  
    VLAN trunking for virtual FortiGate dvSwitch modification .................... 12  
    Static Route Folder Relocated to Device Level ........................................... 12  
    OSPF Mtu-Ignore Option ........................................................................... 12  
    Device Package Version Compatibility ......................................................... 12  
    Fortigate OS Compatibility ......................................................................... 13  
    Predefined keywords ................................................................................... 13  
    Custom Addresses and Services character limitations .............................. 13  
    VDOM name limitations ............................................................................... 13  
    Rule ID sequence and Policy Name .............................................................. 13  
    BGP/OSPF Configuration ............................................................................. 13  
    Transparent Mode and NAT Mode Configuration ......................................... 13  
    Static Route Sequence Number .................................................................. 14  
    Faults Report ............................................................................................... 14  
    Empty Entries under Parameter Folder ...................................................... 14  
  Known issues .................................................................................................... 16  

**Preparing for deployment** ............................................................................. 18  
  Cisco environment prerequisites .................................................................... 18  
  FortiGate environment prerequisites .............................................................. 18  
    Configuration steps for a FortiGate appliance ............................................ 18  
    Configuration steps for FortiGate-VM ......................................................... 19  
    Configuration steps for FortiManager ......................................................... 19  

**Components in the device package** ............................................................. 20  
  Device model or specification ....................................................................... 20  
  Device script .................................................................................................. 20  
  Directory of supporting files ......................................................................... 20  
  Image file or directory ..................................................................................... 20
Modes of operation ................................................................. 22
  Go-Through mode (Layer 2) ........................................ 22
  Go-To mode (Layer 3) .................................................. 22
Multi-tenant, multi-device support ......................................... 23
Deploying features ............................................................. 24
  Deployment modes .......................................................... 24
  Hybrid mode ............................................................... 24
  Customized dynamic EPG ............................................... 26
BGP ............................................................... 28
Security zone ................................................................. 32
Bidirectional forward detection (BFD) ................................... 34
IPv6 ................................................................. 35
Firewall port forwarding (destination NAT) ......................... 38
Device health ............................................................... 41
Interface statistics .......................................................... 41
Dynamic EPG notification ................................................... 42

Deployment procedures ..................................................... 45
  Device package installation ............................................. 45
  Service deployment ..................................................... 45
Importing the device package ............................................. 46
  Remove device package ................................................ 46
Basic steps to add Fortinet firewall L4-L7 virtual device ............ 47
  Add L4-L7 device ........................................................ 47
  Create a functional profile group ..................................... 49
  Create a functional profile ............................................. 49
  Review ........................................................................ 50
Service graph ................................................................. 51
  Create a service graph ................................................... 51
  Deploy service graph .................................................... 52
  Modify a service graph .................................................. 52
  Remove a Service Graph ............................................... 54
  Service graph deployment ............................................... 56

APIC infrastructure and FortiGate rollback ............................. 57

Basic troubleshooting .......................................................... 58
  Verify the service graph deployment .................................. 58
  Service deployed but parameters missing .......................... 59

Use case scenarios ............................................................. 61
  Deploying data center layer 2 segmentation with Cisco ACI and FortiGate .......................... 61
    Prerequisites .............................................................. 61
    Workflow ................................................................. 61
    Configuration ............................................................ 62
  Deploying data center Layer 3 segmentation with Cisco ACI and FortiGate ......................... 67
    Introduction .............................................................. 67
    Prerequisites .............................................................. 67
    Workflow ................................................................. 68
    Configuration ............................................................ 68
  Deploying firewall service for north-to-south traffic with OSPF ..................................... 83
About FortiGate Connector for Cisco ACI

FortiGate Connector for Cisco ACI (Application Centric Infrastructure) is the Fortinet solution to provide seamless integration between Fortinet Firewall (FortiGate) deployments and the Cisco APIC (Application Policy Infrastructure Controller). This integration allows customers to perform single point of FortiGate configuration and Management operation through Cisco APIC.

While the FortiGate series of firewalls enable superb firewall services, in a data center environment, the insertion, configuration, and management of network services such as firewall can be quite complex and potentially error-prone tasks. One solution for such data center problems is Cisco’s ACI. Cisco’s 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 ACI fabric’s leaf node through APIC. Traffic demanding certain network services is steered by APIC-managed policies to the appropriate resources. The FortiGate Connector allows FortiGates to be included amongst the list of resources that traffic can be directed to.

Recommended minimum resources

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

<table>
<thead>
<tr>
<th>Memory:</th>
<th>4 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU:</td>
<td>2 vCPU</td>
</tr>
</tbody>
</table>
About FortiGate Connector for Cisco ACI

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk:</td>
<td>20-50 GB</td>
</tr>
<tr>
<td>vNICs:</td>
<td>1</td>
</tr>
</tbody>
</table>

**Licensing**

FortiGate Connector for Cisco ACI is free of charge for Fortinet customers. You need to make sure that you register your FortiGate with FortiCare on support.fortinet.com.
Supported Fortinet products

The supported Fortinet products refers to those that are compatible with the FortiGate Connector for Cisco ACI software, and will properly integrate into the Cisco ACI. The products are separated into models and firmware but it is an “and” set of parameters. In order to be supported the Fortinet product has to be one of the listed models running supported firmware.

Firmware versions

FortiGate Connector v2.3 for Cisco ACI is compatible with the following FortiOS firmware:

- FortiOS 6.0.2

Models

FortiGate Connector for Cisco ACI v1.3 and above supports the following predefined models:

<table>
<thead>
<tr>
<th>Model</th>
<th>Fortinet Device Package for Cisco ACI v1.3</th>
<th>Fortinet Device Package for Cisco ACI v 2.2</th>
<th>Fortinet Device Package for Cisco ACI v2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco APIC versions:</td>
<td>Cisco APIC versions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.2 (2.x)</td>
<td>3.2 (1m)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.2 (3.x)</td>
<td>3.1 (2o)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.0 (x)</td>
<td>2.2 (3.x)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.1 (2.x)</td>
<td>2.3 (1.x)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.0 (1k)</td>
<td></td>
</tr>
<tr>
<td>FG-300D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-600D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-800D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-900D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-1000C</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-1000D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-1200D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-1500D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-3000D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-3100D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-3200D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>Model</td>
<td>Fortinet Device Package for Cisco ACI v1.3</td>
<td>Fortinet Device Package for Cisco ACI v2.2</td>
<td>Fortinet Device Package for Cisco ACI v2.3</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Cisco APIC versions:</td>
<td>Cisco APIC versions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 1.2 (2.x)</td>
<td>● 3.2 (1m)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 1.2 (3.x)</td>
<td>● 3.1 (2o)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 2.0 (x)</td>
<td>● 2.2 (3.x)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 2.1 (2.x)</td>
<td>● 2.3 (1.x)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>● 3.0 (1k)</td>
<td></td>
</tr>
<tr>
<td>FG-3700D</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-3980E</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-6300</td>
<td>Not supported</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-6500</td>
<td>Not supported</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-7040E</td>
<td>Not supported</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
<tr>
<td>FG-VM</td>
<td>FortiOS 5.4</td>
<td>FortiOS 5.6 &amp; 6.0</td>
<td>FortiOS 6.0.2</td>
</tr>
</tbody>
</table>

**Unlisted models**

Additional models will be added in the future based on customer requests.

---

⚠️ The use of FortiGate Connector can be attempted with any FortiGate model, but do so with caution. Only those listed above have been confirmed. If an unlisted model of FortiGate is used, the user needs to verify port names match the FortiGate model.
Terms and concepts

Application network profiles

An application network profile is a group of one or more end point groups (EPG) and the contracts that define how they communicate. The contracts are used to define the connectivity of application tiers such as web-app-database and compute-network-storage.

Bridge domain (BD)

A bridge domain is a L2 forwarding construct within the fabric that is used to constrain broadcast and multicast traffic. They must be linked to a virtual routing and forwarding object (VRF). Multiple BDs can be associated to a single VRF.

Contract

A contract defines rules such as inbound and outbound permit, deny, and QoS, and policies such as redirect. Contracts are enforced between EPGs using the provider-consumer relationship. One EPG provides a contract, and the other EPGs consume that contract.

End point group (EPG)

EPGs are containers for collections of applications or application components.

- Contract logic is applied to EPGs.
- They allow the separation of network policy, security, and forwarding from addressing and instead apply it to logical application boundaries.
- Grouping is independent of addressing, VLAN, and other network constructs as opposed to traditional network environments that must rely on these for groupings.

FortiGate VDOMs

Virtual Domains are used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.

FortiOS RESTful API

REST (sometimes spelled ReST) stands for Representational State Transfer. It is a software architectural style for the WWW. REST systems typically communication over HTTP, using HTTP verbs or commands to retrieve and send information to remote servers.
A good resource for the finer details of Fortinet’s implementation of ReST can be found at

North-south and east-west traffic

The cardinal compass direction terms to describe traffic flow are used to differentiate between traffic within the cloud or data center and traffic going in and out of the cloud or data center.

- North/south - traffic either heading into or out of a cloud or data center.
- East/west - traffic that is between nodes inside the same cloud or data center.

Tenant

A tenant:

- Is a logical container for application policies.
- Provides RBAC isolation.
- Represents isolation from a policy perspective.
- Can represent a customer in a service provider setting, an organization or domain in an enterprise setting, or just a convenient grouping of policies
- Can be isolated from one another or can share resources. The primary elements that the tenant contains are filters, contracts, outside networks, bridge domains, contexts, and application profiles that contain endpoint groups (EPGs).

The fabric can contain multiple tenants.

Virtual router and forwarding (VRF)

VRFs (also called contexts) are defined within a tenant to allow:

- L3 isolation.
- Potentially overlapping IP address spaces.

Special notice

Service manager mode: AutoPush feature interact with zoning

If a user is configured to use zone in conjunction with the AutoPush feature, the zone information will not appear on any FortiGate(s) until the policy is pushed out to them.
VLAN trunking for virtual FortiGate dvSwitch modification

After a service graph is deployed using this feature, you need to modify the ACI dvSwitch vNIC mapping to the FortiGate-VM as well as changing the port group mode to trunking in order for the traffic to forward.

Static Route Folder Relocated to Device Level

Due to Cisco’s recommendation to accommodate multiple service graphs with PBR use case, we have moved the Static Route Folder to the Device Level. Please see below screenshot.

OSPF Mtu-Ignore Option

When enable MTU-Ignore option for OSPF Configuration, Cisco ACI will push down mtu size of 1 which caused the programming of OSPF interface and network on the Fortigate to fail (Mantis 0502409). Please skip using this option for now until Cisco has resolved this issue.

Device Package Version Compatibility

This device package is not backward compatible with release 1.3.x Device Package or early release of 2.x. Any configuration that was done using Device Package 1.3.x or early release of 2.x will not be importable into this release.
Fortigate OS Compatibility

We have tested FortiOS 6.0.2 for this release.

Predefined keywords

Do not modify the predefined key words used by FortiGate.

Custom Addresses and Services character limitations

The name fields of Firewall Addresses and Services should not include spaces or special characters.

VDOM name limitations

Beginning with FortiGate Connector v1.2, VDOM name is no longer a configurable option due to design recommendation from Cisco. The VDOM name will be the virtual device ID. After a service graph is deployed, a virtual Device ID is randomly assigned by Cisco APIC and that will be the VDOM name appears on Fortigate. However, in the VDOM name comments field it will display the ACI Tenant information so customer can get an idea between Tenants to Vdom association.

Rule ID sequence and Policy Name

Rule ID with lowest number will get processed and listed first on the FortiGate. In addition, if deploying multiple service graphs shared with same virtual device, please ensure Rule IDs and Policy Names are unique otherwise, they will override each other.

BGP/OSPF Configuration

User doesn’t need to perform any BGP/OSPF parameter configuration except Router ID configured in Router Configurations under L4-L7 services. The recommendation from Cisco is that user creates BGP/OSPF Configuration on L3OUTs which is the corresponding interface configuration along with all BGP/OSPF parameters to the FortiGate on APIC. During the Service Graph deployment, Fortigate Connector device package will extract the BGP/OSPF parameters from APIC and then program the corresponding BGP/OSPF configurations on FortiGate.

Transparent Mode and NAT Mode Configuration

Beginning with FortiGate FortiConnector v1.2, the device package no longer has the option to select VDOM mode. When Go-Through mode is selected, interface ip address field must be in default setting; when “GoTo” mode is selected, interface ip addresses must be configured with valid ip address and network mask. This restriction however lifted as of Cisco ACI v2.0(2i).
Static Route Sequence Number

For Static Route Sequence Number of 0 (default value), Device Package will ignore static route programming. Otherwise, Device Package will program any entry in the Static Route fields when Sequence Number is greater than 0.

Faults Report

When Device Package returned fault(s) to Cisco ACI due to various reasons, the fault message(s) will show up in Cisco ACI System level instead of Tenant level. However, you will still see the fault from the debug.log file.

We also observed on some occasion when we report fault code to Cisco ACI, but ACI will not show up nor will it take any action. The work around would be to remove the service graph and redeploy again.

Empty Entries under Parameter Folder

There is an issue we found when we leave Folder/Parameter fields empty when they previously have existing entries. The device package will not be able to fallback to default value which caused no update for those Parameter(s). Example: We applied a Service Graph with Customer Firewall Address Group by selecting “Show in Address List” option to be “enable”. If we clear this field by clicking on the “x” box (Figure 1) will result in clearing all options within it (Figure2). By clearing this field, the default value should be “disable” but our device package will not be able to handle it. The work around is to changing the option from “enable” to “disable” instead of leaving the field empty. This behavior will affects all other Folder/Parameter until we fix it in later release.
Figure 1

Clicking on X box will clear all entries
Known issues

The following issues have been identified in version 2.3. For inquiries about a particular bug or to report a bug, please contact Customer Service & Support.
<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>380069</td>
<td>When there is a Service Graph generated Fault, the Fault message will display at System Level instead of Tenant Level. Cisco has been notified on this issue.</td>
</tr>
<tr>
<td>403172</td>
<td>Administrative priority from static route cannot add value to 4294967295. Cisco ACI only supports up to 9 Digital entries.</td>
</tr>
</tbody>
</table>
Preparing for deployment

Because this software connects two products or environments that are produced by different companies, care must be taken to make sure that both sides are compatible with both the connection software and each other.

Cisco environment prerequisites

Before the Fortinet Device Package for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied within the Cisco environment.

One of the following Cisco ACI environments needs to be in place:

- Cisco ACI v3.2.(1m)

Within the Cisco ACI, the following configurations need to be completed before deploying Layer 4 -7 Services such as the FortiGate Connector.

- Creation of access policies configuration under the Fabric menu
- Creation of required tenant(s)
- Creation of network(s) (including Bridge Domain)
- Creation of application profile(s)
- Creation of end point group(s)
- Creation of contract(s)
- Creation of BG/OSPF L3Out (if required)


Pre-existing L4-L7 configurations based on FortiGate Connector v1.3 or v2.x are not compatible. They will need to be reconfigured.

FortiGate environment prerequisites

Before the FortiGate Connector for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied on the FortiGate side of the equation. The configuration steps can vary depending on whether you are connecting a physical appliance or a virtual version of the FortiGate.

Configuration steps for a FortiGate appliance

1. Configure an administrator user name and password.
2. Enable HTTP and/or HTTPS on MGMT port.
3. Configure the IP address for the MGMT port.
4. Enable VDOM-Admin globally.
5. Configure Port-Group if required.

**Configuration steps for FortiGate-VM**

1. Assign network ports before starting the VM.
2. Configure an administrator user name and password.
3. Enable HTTP and/or HTTPS on the MGMT port.
4. Configure the IP address for the MGMT ports.
5. Enable VDOM-Admin globally.

**Configuration steps for FortiManager**

Before the Fortinet Device Package can be successfully deployed, a number of prerequisites need to be satisfied on the FortiManager side of the equation.

1. Configure administrator user name and password.
2. Enable HTTP and/or HTTPS on the MGMT port.
3. Configure the IP address for the MGMT ports.
4. Register any FortiGate(s) with FortiManager.
Components in the device package

To add a network service to the ACI fabric, upload the device package for the service to APIC. The device package is a zip file containing these components:

Device model or specification

The device specification is an XML file called DeviceModel.xml that covers descriptions of FortiGate devices, interfaces, connectivity and services. The file contains a hierarchical description of FortiGate devices, including:

- Device functions
- Parameters of each function
- Interfaces/network connectivity information of each function

Device script

This is a Python file, DeviceScript.py with API functions to interface between the Cisco APIC and the FortiGate REST APIs. This Python file is associated by the DeviceModel.xml device specification to the device script for APIC.

Directory of supporting files

This component contains supporting Python files, text files and libraries of scripts and tools.

Image file or directory

The directory contains file(s) such as a Fortinet icon (Fortinet_name.gif) which is displayed on the APIC management page.
**Modes of operation**

Cisco APIC integrates with two types of devices. The devices are defined by their mode of operation: either Go-Through or Go-To. You should determine which mode of operation you intend to use before installation as it can have an impact on how you set up the logical topology of the network.

**Go-Through mode (Layer 2)**

Devices in Go-Through mode are considered layer 2 devices (from the OSI model) and are sometimes known as transparent. They are referred to as transparent because while the traffic goes through them and can be affected by them, they are not seen by the network and are not a destination in their own right for the traffic. They do not route traffic. These devices are not referred to by the packet’s destination MAC or IP address. In most cases, these devices will only have an address for the purposes of management.

**Go-To mode (Layer 3)**

Devices in Go-To mode are considered Layer 3 (from the OSI model) devices. They can route traffic and they are referenced as the destination in a packet’s destination MAC address or destination IP address.
Multi-tenant, multi-device support

- Multi-tenant, multi-device is a typical use case. After a FortiGate device is added to a tenant’s L4-L7 services, the multi-context aware setting can be enabled. This indicates to the device package that the L4-L7 device is going to be a virtual device that shares its resources with other tenants on the FortiGate. In FortiGate implementation, this virtual device is represented by a VDOM. Multiple virtual devices can be configure under each tenant. The VDOM name is the virtual device ID generated by APIC when a virtual device is added.

- Each tenant sees all available interfaces and can share interfaces (ports) with other tenants, if it is multi-context aware. For Physical Device under L3 Routed (Go-To) mode, the tenant can share a physical interface as the VLAN is used to isolate the physical interface. In a VM Device, this is not true. You can only use a dedicated VNIC.
Deploying features

Because of the wide variation in environments and the wide range of networking requirements, there are a number of features available that can be used in the deployment and its configuration.

Deployment modes

This table shows the various modes and related requirements of Cisco-ACI deployment.

<table>
<thead>
<tr>
<th>Deployment mode</th>
<th>Network configuration</th>
<th>FortiGate configuration</th>
<th>Device package</th>
<th>EPG visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed</td>
<td>From APIC</td>
<td>From APIC</td>
<td>Required</td>
<td>EPG in Service Graph</td>
</tr>
<tr>
<td>Hybrid</td>
<td>From APIC</td>
<td>Manual</td>
<td>Required</td>
<td>EPG in Service Graph</td>
</tr>
</tbody>
</table>

Hybrid mode

Hybrid mode configuration

We now support Hybrid Mode which allows our device package to automate network configuration (Device Interfaces, Security Zone, Static Route, and BGP/OSPF) and Dynamic EGP feature (Address Group) through Cisco ACI but yet reserve the flexibility of controlling the Firewall configuration for the end user on the FortiGate.

The Fortinet definition of Hybrid mode is not the same as Cisco's definition of Hybrid mode, which is referred to in https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-734587.html. Cisco refers to this mode in their documentation as Service Manager mode. Fortinet refers to it as Hybrid mode because of its hybrid character of having aspects of both Managed and Unmanaged modes.

Customers who modify or add any other non-networking or Dynamic EPG (Address Group) options will get ignored by Cisco ACI in case of service auditing.

If customers want to use non-hybrid mode, the behavior is same as existing device package.
The new Hybrid mode option is under the VDOM-Folder. It is recommended that you not toggle between hybrid and non-hybrid mode once you made the selection. To avoid changing it at later stage, it is best to check the Locked Field to "Lock" this option from modification once it is deployed.

As far as networking aspect of the configuration, “Device Interface”, “Security Zone” “Static Route”, and “BGP/OSPF”, they are the same as existing device package.

If you want to remove the service graph, ensure that you manually remove any associated FortiGate-side firewall configurations before removing the graph. If this is not done first, the ACI will not be able to remove the interfaces/VDOM.
Device interface configuration

Static route configuration

Customized dynamic EPG

If you wish to create your own customized EPG group name, you need to first define an address group under the IPv4 Firewall Address Group folder and then apply the newly defined group to the VDOM Interface consumer/provider Addrgrp level. This feature will function under Hybrid and Non-hybrid mode.
To enable this feature, VDOM Interface Consumer Addrgrp and VDOM Interface Provider addgrp have been added to the VDOM Folder level.

By default, there are two prepopulated group called cons_dyn_epg_grp and prov_dyn_epg_grp which represent consumer and provider EPG groups respectively.

Define customized dynamic EPG group
Apply the customized address group

You are advised to lock this field. If you change the mapped group once it is deployed, the end point member(s) will be shown in both the old and new address groups.

The dynamic EPG function that was introduced in FortiGate Connector v1.3 will no longer work. You will have to use this method moving forward.

BGP

For this release, we completed our dynamic routing protocol suite by supporting BGP. Similar to OSPF, we take configuration from Cisco ACI L3Out with BGP configuration and program FortiGate accordingly. Please note that only iBGP is supported based on Cisco ACI’s supportive matrix. Configuring ACI L3Out is beyond the scope of this document, however below are some screenshots which can guide you through the configuration.

Create the L3 outside

Define:

- vrf name
- routed roomain
- routing protocol
Create a node profile under L3 outside

Define the node information as well as the BGP peering information.

Create L3 outside interface profile

Define the L3 out interface information.
Create L3 outside BGP peering connection

For IBGP, there is no need to define Remote AS Number. The Local AS number is taken from the Route Reflector AS number. (For details on how to configure Route Reflector AS Number, please consult Cisco ACI document.)
Create L3 outside OSPF interface profile and profile policy if OSPF is used

Create L3 outside route ID
Create L3 outside network

Security zone

Enable the Security Zone feature by going to Function Config > Network > Device Interface Zone and selecting External or Internal under the default xml. By default it is disabled with member “none” (Figure1). To enable security zone, select the corresponding interface from the member drop down list. (Figure2).

If customer is using Full Managed mode and security zone is enabled, policy rule(s) will follow the interface/zone behavior. Ex: If user selected to use security zone for internal and external then the policy rules will be programmed between internal and external zones.

To customize the zone name, user simply changes the name under the Name Column. The default names are “Interfacezone-external” and “Interfacezone-internal”.

Before pushing the service graph, ensure that no interface exists on multiple zones. This is to avoid a configuration error because one interface can only belong to one zone at a time.

Figures 3 and 4 are sample output of security zone deployed in interface and policy screen within the FortiGate.
Components in the device package

Figure 1

![Figure 1](image1.png)

Figure 2

![Figure 2](image2.png)
Bidirectional forward detection (BFD)

BFD is a feature for dynamic routing, which Cisco ACI does not provide to the FortiGate, when any dynamic routing protocol is involved. To accommodate this, enabling BFD is an option under the Device interface level. By default, the...
option is turned off.

**IPv6**

**IPv6 interface configuration**

We now support IPv6 configuration on the interface level.
IPv6 policy

After you have configured the IPv6 addresses onto the interfaces, you can configure an IPv6 policy to enforce the traffic.

IPv6 DoS

Optionally, you can configure the IPv6 DoS feature.
IPv6 virtual IPs

In addition, you can configure the IPv6 Virtual IP feature, which you can apply to an IPv6 policy.
Firewall port forwarding (destination NAT)

IP pool configuration

The table and screenshot below illustrate how to define an IPv4 IP pool. Due to the layout format ACI provides, you have to list all the sub-features within the IP pool. Consult the FortiGate Configuration Guide for options that go with appropriate sub-features. Otherwise, you will see an error when you push the configuration from the APIC down to the FortiGate. The table shows the sub-features and the options.

<table>
<thead>
<tr>
<th>Dynamic IP pool</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Pool type</td>
<td>IPv4 pool</td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Comments</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Overload</td>
</tr>
<tr>
<td>External IP range</td>
<td>x</td>
</tr>
<tr>
<td>Internal IP range</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Dynamic IP pool

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Block size</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>x</td>
</tr>
<tr>
<td><strong>Blocks per user</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>x</td>
</tr>
<tr>
<td><strong>ARP reply</strong></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### IPv4 virtual IPs

IPv4 virtual IP pools can also be configured for DNAT.
Enable DNAT on the policy

After DNAT sub-components are configured, you can apply them to the policy level.
Device health

From the L4-L7 Device level, you can obtain the FortiGate device health. Go to L4-L7 Services > L4-L7 Devices > Device Name > Concrete Device > Health Tab.

Interface statistics

From the L4-L7 Device level, you can also obtain the FortiGate interface statistic. Navigate to L4-L7 Services > L4-L7 Devices > Device Name > Concrete Device > Interface > Stats Tab. Here you can see the interface statistics by enabling the various statistics indicators such as RX/TX, and so on.
Dynamic EPG notification

This feature allows you to dynamically update the object group membership, where it corresponds to an endpoint group (EPG). You can dynamically add IP addresses/subnets based on an endpoint/network attachment notification by ACI.

There are two groups, "dyn_epg_ext_grp" and "dyn_epg_int_grp", to which you can apply to the policy source field. When an endpoint is detected, a notification is received from ACI and the endpoint IP is added to the membership group where the policy is applied.

In the above example, "dyn_epg_int_grp" is added to the Source Address Group Name field under Policy 10.
From L4-L7 Service Graph Template > Function Node > Consumer/Provider, you must check the box Attachment Notification in order for ACI to notify the FortiGate when the endpoint is attached to the group.
EPG operational level indicated endpoint attached to the EPG
Deployment procedures

The following sections describe the procedures for deploying a service insertion.

Device package installation

To successfully deploy FortiGate Connector into Cisco APIC, you need to perform the following steps:

1. Import the device package
2. Add an L4-L7 device
3. Create a functional profile
4. Create a service graph template
5. Deploy the service graph template

Service deployment

According to the APIC deployment guide, this is the typical procedure to have a service device introduce a Layer 4 to Layer 7 service:

1. Import the device package for the service device
2. Configure a tenant that requests network services
3. Register the device and its logical interfaces
4. Configure the logical device parameters
5. Configure a layer 3 network
6. Configure a bridge domain
7. Configure an application profile
8. Configure a physical domain (or VMM domain)
9. Configure a VLAN pool
10. Configure a contract
11. Configure a management endpoint group (EPG)
12. Configure a service graph template
13. Select default service graph template parameters
14. Attach the service graph template to a contract
15. Configure additional configuration parameters

To add support for a non-Cisco firewall device in the Cisco ACI fabric based data center, a device package needs to be developed for the APIC. Then perform the standard APIC deployment of a network service device.
## Importing the device package

1. Download the device connector package from the Fortinet Support website to local storage.
2. From the APIC menu, go to L4-L7 Services > Packages and right click on L4-L7 Device Type on the left hand panel. Select Import Device Package.

![Importing the device package](image)

## Remove device package

To remove device package, go to L4-L7 Services > Packages and right click on the device package on the left panel and select Delete option.
Basic steps to add Fortinet firewall L4-L7 virtual device

Add L4-L7 device

Within the Tenant, expand L4-L7 Services > L4-L7 Devices, then right click on Create L4-L7 devices.
**General**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description / options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Device</td>
</tr>
<tr>
<td>Device Package</td>
<td>Select Device Package</td>
</tr>
<tr>
<td>Model</td>
<td>&lt;List of the supported models&gt;</td>
</tr>
<tr>
<td>Mode</td>
<td>• Single Node / HA Cluster</td>
</tr>
<tr>
<td>Function Type</td>
<td>• GoThrough (L2)</td>
</tr>
<tr>
<td></td>
<td>• Goto (L3)</td>
</tr>
</tbody>
</table>

**Connectivity**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description / options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Domain or VMM Domain</td>
<td>Select the domain which you should have configured during APIC Access Policies setup</td>
</tr>
<tr>
<td>APIC to Device</td>
<td>• Out-of-Band</td>
</tr>
<tr>
<td></td>
<td>• In-Band</td>
</tr>
</tbody>
</table>

**Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>&lt;login name to the FortiGate&gt;</td>
</tr>
<tr>
<td>Password</td>
<td>&lt;Password to log in to FortiGate&gt;</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>&lt;Password to log in to FortiGate&gt;</td>
</tr>
</tbody>
</table>

**Device 1**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description / options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP Address</td>
<td>&lt;IP address to connect to FortiGate&gt;</td>
</tr>
<tr>
<td></td>
<td>• http</td>
</tr>
<tr>
<td></td>
<td>• https</td>
</tr>
<tr>
<td>Management Port</td>
<td>https is the preferred method</td>
</tr>
<tr>
<td>Connects To</td>
<td>• Port (Default), PC, VPC</td>
</tr>
<tr>
<td>Physical Interfaces</td>
<td>Click on “+” sign to add interfaces connecting from APIC to FortiGate</td>
</tr>
<tr>
<td>Name</td>
<td>Select a port.</td>
</tr>
<tr>
<td></td>
<td>(If using Port Channel, type the Port Channel name ex: PO1, PO2..etc.)</td>
</tr>
</tbody>
</table>

**Cluster**

Configure all fields the same as Device 1, except for the Cluster Interface.

For the cluster interface, click the “+” icon to add logical device interfaces.
Create a functional profile group

![Image of functional profile group creation](image1)

Remove a functional profile group

To remove a functional profile group, go to Tenant > L4-L7 Services > Functional Profiles, and right click on the functional profile group name listed on the left hand panel and select Delete.

![Image of functional profile group deletion](image2)

Create a functional profile

1. Navigate to the Functional Profile group you created. Right click Create L4-L7 Service Functional Profile.
2. Input the functional profile name, and leave the Copy Existing Profile Parameters option checked. In the Profile field, select Fortinet-FGAPIC-1.0/Basic-Firewall-Policy.

Review

The All option displays all the fields in the features listing. If you are satisfied with all your settings, click on the SUBMIT button to complete your creation of the functional profile template.
Service graph

Create a service graph

The service graph template is used to tightly couple the functional profile or firewall configuration, and combine it with the firewall device you defined in the earlier steps.
Right click on L4-L7 Service Graph Template to create a service graph.

**Deploy service graph**

After you combine the firewall configuration and associated device, you can deploy the service graph to automatically create a VDOM.

Right click on the service graph defined earlier and select Apply L4-L7 Service Graph Template.

**Modify a service graph**

1. Go to Tenant > Provider EPG > L4-L7 Service Parameters and select the pen icon. This activates the edit mode used to modify parameters on a deployed service graph.
2. On the next screen, select the Contract Name, Graph Name and Node Name from the drop down list. This displays all of the associated service graph parameters.

3. Expand the field you want to make the modifications to and change the appropriate value from the drop down list. Save the changes by clicking on the SUMBIT button.
Remove a Service Graph

1. Go to Tenant > L4-L7 Services > L4-L7 Service Graph Templates. Right click on Service Graph template and select Remove Related Objects Of Graph Template.

2. Select Contract and Provider EPG from the drop down list and check all 3 boxes:
   - Remove Related Contract
   - Remove Related EPG Parameters
   - Remove Related Device Selection Policies

   Hit the SUBMIT button. This removes all of the related objects for this service graph.
Delete the service graph

1. To delete a service graph template, go to Tenant > L4-L7 Services > L4-L7 Service Graph Templates.
2. Right click on template name listed on the left hand panel and select Delete.
Service graph deployment

After the service graph is deployed, the FortiGate device receives configuration updates through REST API commands from the Cisco APIC. The figure below shows a successful service graph deployment. The interface configurations such as VLAN, IP, and so on, as well as firewall policies are all programmed onto the FortiGate. From this point forward, any update is continually managed by the Cisco APIC until the service graph is removed.
In order to rollback a FortiGate deployment with the APIC infrastructure, these are the basic steps:

1. Upload and unload device package
2. Add and delete the device. The FortiGate should clean-up previous configuration.
3. Dynamically modify and update policies
4. Detach and attach service graphs
5. Delete tenants while service graphs in use.
Basic troubleshooting

Verify the service graph deployment

If the service graph deployment failed:

- Go to Tenant > Deployed Graph Instances to check the state of the deployed graph.
- If the state is failed apply, go down one level to the Deployed Graph Instances and select the Fault tab to check the error log. Any error codes in the 1000 range relate to the FortiGate. Other codes refer to APIC.

Currently we only have the following error codes:

<table>
<thead>
<tr>
<th>Error code</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1010</td>
<td>Configuration Error in device configuration</td>
</tr>
<tr>
<td>1020</td>
<td>Configuration Error in function configuration</td>
</tr>
<tr>
<td>1030</td>
<td>Internal Error -3</td>
</tr>
<tr>
<td>1040</td>
<td>Internal Error -4</td>
</tr>
<tr>
<td>1050</td>
<td>Internal Error -5</td>
</tr>
<tr>
<td>1070</td>
<td>Feature not available</td>
</tr>
</tbody>
</table>
Service deployed but parameters missing

If the service deployed, but certain parameters not showing up on the FortiGate, perform the following steps:
1. Go to Tenant > Provider EPG > L4-L7 Parameters. Ensure that the missing parameters are listed. If they are not listed, double check the functional profile to confirm the configuration.

Figure 1

2. If they are listed, log in to the Cisco APIC controller to examine the debug log. The debug log is located at /data/devicescript/Fortinet.FGAPIC.(version number)/logs and the log file name is debug.log. Examine the log file and grab fields with the format [10.160.11.103, <xxxx>]: and scan through the logs associated to the parameters in question.

3. If none of these steps lead to an answer, send the entire captured log to the Fortinet Technical Assistance Center for further troubleshooting.
Use case scenarios

Some information about the deployment or configuration of software can be a little abstract, so a number of use case scenarios have been included to show the variations in how to use the information in more specific and practical situations.

Deploying data center layer 2 segmentation with Cisco ACI and FortiGate

Prerequisites

- Create the following Security Fabric policies:
  - VLAN pools
  - Domain
  - Attachable Access Entity profiles
  - Interface policies
  - Switch policies
- Create tenant, VRF, 2 bridge domains, 2 EPGs
- Associate the 2 bridge domains to VRF
- Associate the 2 EPGs to the 2 bridge domains
- Import the Layer 4-7 Device Package into Cisco APIC

Workflow

1. Create a L4-L7 device with Go-through mode
2. Create a functional profile
3. Create a service graph template
4. Deploy a service graph
Configuration

Create a L4-L7 device with Go-Through mode on Cisco APIC

Create a functional profile

The functional profile defines the template for any services that are deployed, such as L4-L7 device interface IP addresses, rule ID, object addresses, policy rules, source/destination ports.
**Explanation of functional profile objects**

**Device configuration**

The device configuration contains external and internal interfaces that are programmed into the FortiGate VDOM. These are the interfaces (typically external and internal) that are associated to the VDOM. If you intend to have multiple link deployment scenarios, this is where additional interfaces with unique names can be added.

![Tip icon] Leave the IP address field untouched in Go-Through mode.

**Function configuration**

Function configuration consists of:

- **Network**
  - Use this field to configure static routes for IPv4 and IPv6.
- **Policy and objects**
  - This folder is the container for the following folders:
    1. FWServiceFolder – Firewall service object container
    3. IPv4/IPv6 FirewallAddresses – Firewall addresses object container
    4. IPv4 Policy – Firewall policy rule container
    5. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
    6. ScheduleFolder – Schedule container
- **VDOM-folder**
  - VDOM internal and external interfaces

**Create the service graph**

The service graph template is used to tightly couple the functional profile or firewall configuration and combine with the firewall device.
Deploy the service graph

Once you combine the firewall configuration and associated device together, deploy the service graph.

On the next screen, select the Consumer and Provider EPGs and assign a contract name or select a pre-defined contract.
On the next screen, select the logical interfaces defined during the creation of the L4-L7 device.

On the next screen, validate all configurations before deployment. If everything is correct, click on the Finish button.
Deploying data center Layer 3 segmentation with Cisco ACI and FortiGate

Introduction

This use case scenario describes the configuration of an L4-L7 service graph with L3 segmentation within a data center.

Prerequisites

- Create fabric access policies relating to:
  - VLAN pools
  - Domain
  - Attachable access entity profiles
Use case scenarios

- Interface policies
- Switch policies
- Import the L4-L7 device package into Cisco APIC

**Workflow**

1. Create the tenant (TenantB in our example)
2. Create VRFs (VRF1 and VRF2 in our example)
3. Create the bridge domains and map to VRFs (Bridge Domain App and DB are mapped to VRF1 and VRF2 respectively in our example)
4. Create EPGs and map them to the bridge domains (EPG-DB and EPG-App in our example)
5. Create two L3 outside EPGs (1 for Firewall External and 1 for Firewall Internal. In this example, “FortigateExternalOut” is used for Firewall External and “FortigateInternal” for is used Firewall Internal)
6. Configure the gateway IPs on bridge domains (DB and App) for App and DB Servers
7. Ensure “Unicast Routing” is enabled in each bridge domain
8. In Bridge Domain App, associate the L3 outside to “FortigateExternalOut”; and in Bridge Domain DB, associate the L3 outside to “FortigateInternal”
9. Map the App and DB machines to EPGs and configure the correct IP addresses, and use Bridge Domain IP address (configured in step 6) as its gateway
10. Verify that the App and DB machines can reach (ping) the gateway IP address
11. Create the L4-L7 device in the GoTo mode
12. Create a functional profile group as well as a functional profile
13. Create the route profiles
14. Create the L4-L7 service graph template
15. Deploy the L4-L7 service graph

**Configuration**

**Configure the bridge domain DB and App as well as VRF1 and VRF2**

Associate bridge domain App to VRF1 and bridge domain DB to VRF2.
Configure the L4-L7 device for the physical FortiGate (Go-To mode)
Configure the L3 outside for FortiGate external interface and associate with VRF1

Configure the SVI for L3 outside FortiGate external out
Configure the route ID for L3 outside FortiGate external out

Configure the import/export route control on the subnets for the FortiGate external out
Configure the L3 outside for the FortiGate internal and associate with VRF2

Configure the SVI for L3 outside FortiGate internal
Configure the route ID for L3 outside the FortiGate internal

Configure the import/export route control on the subnet for L3 outside FortiGate internal
Associate the EPG “DB” to bridge domain “DB” and attach the bridge domain to VRF2
Configure the bridge domain with unicast routing, assign SVI and associate L3 outside to “FortigateInternal”

Associate EPG “App” to bridge domain “App” and attach bridge domain to VRF1
Configure the bridge domain with unicast routing, assign SVI and associate L3 outside to “FortigateInternal”
Create a functional profile group and functional profile from existing template
Create a service graph template

Create a router ID that will be used on the service appliance (FortiGate)
Deploy the service graph

Consumer is the App EPG. Provider is the DB EPG.

Select for the internal and external connections. In this example, "FortigateExternalOut" and FortigateInternal are used as external and internal selections respectively.
Use case scenarios

Verify the configuration, then click “Finish”
Check the status and verify device selection policy
Use case scenarios

Verify the deployed graph instance

FortiGate Connector for Cisco ACI Deployment Package
Deploying firewall service for north-to-south traffic with OSPF

Introduction

This use case scenario describes the configuration of an L4-L7 service graph with route peering, where the consumer is external to the ACI fabric and the provider is internal to the Cisco ACI Fabric. With the route peering feature by Cisco APIC enabled, the external traffic can reach internal servers through L4-L7 services.

Prerequisites

- Create fabric access policies relating to:
  - VLAN pools
  - Domain
  - Attachable access entity profiles
  - Interface policies
  - Switch policies
- Create a Layer 3 connection outside of the ACI fabric
- Import the L4-L7 device package into Cisco APIC
Workflow

1. Configure the routing on the external router that is attached to the ACI fabric
2. Create the tenant (TenantB in our example)
3. Create the VRFs (VRF1 and VRF2 in our example)
4. Create the bridge domain and map it to VRF2 (TenBDB in our example)
5. Create the EPG “EPG-DB2” and map it to the bridge domain “TenBDB”
6. Create three L3 outside EPGs:
7. 1 for external connection - In this example, “N5k-1”
8. 1 for firewall external - In this example, “FortigateExternalOut”
9. 1 for firewall internal - In this example, “FortigateInternal”
10. Create the gateway IP on bridge domain (TenBDB) for VM server
11. Ensure “Unicast Routing” is enabled on the bridge domain “TenBDB”
12. In the bridge domain “TenBDB”, associate the L3 outsides to “FortigateInternal”
13. Map the VM server to EPG “EPG-DB2” and configure the IP address and gateway ip address (TenBDB ip address)
14. Verify that the VM server can connect (ping) to the gateway IP
15. Create the L4-L7 device
16. Create a functional profile group as well as a functional profile
17. Create the route profiles
18. Create a L4-L7 service graph template
19. Deploy a L4-L7 service graph

Configuration

Configure the bridge domain TenBDB, VRF1 and VRF2.

Associate bridge domain TenBDB to VRF2
Use case scenarios

Configure the L4-L7 device for the physical FortiGate (Go-To mode)

Configure the L3 outside for N5K-1 and associate to VRF1

All the L3 outside interfaces which are used for route peering are required to be configured as an SVI with VLAN encapsulation accordingly.
Configure SVI for L3 outside N5k-1
Configure the route ID (101.0.0.105 in the example)

Configure the import/export route control on subnets for N5k-1 L3Out external EPG
Configure the L3 outside for the FortiGate external interface (FortigateExternalOut) and associate with VRF1

In this example, the route ID must be the same as above (101.0.0.105), since both L3 outsides are on the same leaf switch.

Configure SVI for the L3 outside FortiGate external out (FortigateExternalOut)
Configure the route ID for the L3 outside FortiGate external outside (FortigateExternalOut)

Configure the import/export route control on subnets for the FortiGate external outside
Configure L3 outside for the FortiGate internal (FortigateInternal) and associate with VRF2

Configure SVI for L3 outside FortiGate internal (FortigateInternal)
Configure the route ID for the L3 outside FortiGate internal (FortigateInternal)

Configure the import/export route control on subnet for L3 outside FortiGate internal (FortigateInternal)
Associate EPG “DB2” to the bridge domain “TenBDB” and attach the bridge domain to VRF2
Configure the bridge domain with unicast routing, assign SVI and associate L3 outside to “FortigateInternal”

Create a functional profile group and a functional profile from the existing template
Create a service graph template
**Create a router ID for the service appliance (FortiGate)**

**Deploy the service graph**

Consumer will be the L3 outside facing external router. Provider is the internal EPG. In this example they are N5k-1 and DB2 respectively.
Route peering must be selected for internal and external connections. In this example, “FortigateExternalOut” and “FortigateInternal” are used as external and internal selections respectively.
Verify the configuration and then click Finish

Check the status and verify the device selection policy
Use case scenarios

Verify the deployed graph instance
Deploying a high availability service with Cisco ACI and FortiGate

Prerequisites

On FortiGate

- Configure the FortiGate HA pair (Active-Standby mode). Please consult Fortinet support website for setting up HA procedures.

On APIC

- Create fabric access policies relating to:
  - VLAN pools
  - Domain
  - Attachable access entity profiles
  - Interface policies
  - Switch policies
- Create the tenant, VRF, 2 bridge domains, and 2 EPGs
- Associate the 2 bridge domains to VRF
- Associate the 2 EPGs to the 2 bridge domains
- Import the L4-L7 device package into Cisco APIC
Workflow

1. Configure Go-Through mode with HA enabled, then configure device #1 and device #2 on Cisco APIC
2. Create the functional profile
3. Create the service graph template
4. Deploy the service graph

In general, the procedures to deploy a Go-Through mode HA scenario vs regular Go-Through mode deployment are identical with the exception of enabling HA during the L4-L7 device configuration. You need to select HA Cluster instead of Single Node for mode selection. Two devices appear on the screen where you input the same Active FortiGate IP address and the corresponding connection ports between FortiGates and Cisco APIC for both devices.

Deploying the firewall service with FortiGate-VM and VMware

Prerequisite

- Create fabric access policies relating to:
- VLAN pools
- Domain
- Attachable access entity profiles
- Interface policies
- Switch policies
- Create the tenant, VRF, 2 bridge domains, and 2 EPGs
- Associate 2 bridge domains to VRF
Use case scenarios

• Associate 2 EPGs to the 2 bridge domains
  • Import Layer 4-7 device package into Cisco APIC

Workflow

1. Create Go-Through mode FortiGate VM devices on Cisco APIC
2. Create a functional profile
3. Create a service graph template
4. Deploy the service graph

Configuration

Create a Layer 4-L7 device on Cisco APIC

Create a functional profile

The functional profile defines the template for any services that are deployed, such as L4-L7 device interface IP addresses, rule ID, object addresses, policy rules, source/destination ports…etc.
Functional profile objects explanation

Device configuration

This scenario requires external and internal interfaces to be programmed into the FortiGate VDOM. These interfaces (typically external and internal) need to be associated with the VDOM.

For Go-To mode, modify the IP address field, or leave the default for Go-Through mode.

Function configuration

Function configuration consists of:

- **Network**
  - Use this field to configure static routes for IPv4 and IPv6.
- **Policy and objects**
  - This folder is the container for the following folders:
    1. FWServiceFolder – Firewall service object container
    3. IPv4/IPv6 FirewallAddresses – Firewall addresses object container
    4. IPv4 Policy – Firewall policy rule container
    5. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
    6. ScheduleFolder – Schedule container
- **VDOM-folder**
- VDOM internal and external interfaces
Create the service graph

The service graph template is used to tightly couple the functional profile or firewall configuration and combine with the firewall device.

![Service Graph Template](image)

Deploy service graph

Combine the firewall configuration and associated device together, then deploy the service graph to create a VDOM.

![Service Graph Deployment](image)

On the next screen, select the consumer and provider EPGs and assign a contract name, or select a pre-defined contract.
On the next screen, select the logical interfaces defined during the creation of the Layer 4-7 device.

On the next screen, verify that everything is configured accordingly before deployment. If the configuration is acceptable, click on the Finish button.
Deploy the firewall device shared by multiple service graphs

Prerequisites

- Create the fabric access policies relating to:
  - VLAN pools
  - Domain
  - Attachable access entity profiles
  - Interface policies
  - Switch policies
  - Import the Layer 4-7 device package Cisco APIC

Workflow

1. Create a tenant ("Tenant1" in the example)
2. Create a VRF ("ctx" in the example)
3. Create 4 bridge domains ("BD1", "BD2", "BD3" and "BD4" in the example)
4. Associate the bridge domains to VRF
5. Create 4 EPGs. The ones used in the example are:
6. "App"
7. "App2"
8. "DB"
9. "DB2"
10. Associate EPGs to bridge domains
Use case scenarios

11. Create a Go-Through mode device on Cisco APIC and define 4 logical interfaces
12. Create a functional profile
13. Create 2 service graph templates
14. Deploy a service graph 2 times on the same device but with different EPG pairs

Configuration

Create the tenant, VRF and 4 bridge domains on Cisco APIC
**Create 4 EPGs**

1. “App” to “BD1”
2. “App2” to “BD2”
3. “DB” to “BD3”
4. “DB2” to “BD4”

**Associate the EPGs to the bridge domains**
Create a device in Go-Through mode with 4 logical interfaces on Cisco APIC

- “Ins” and “Out” for service graph 1
- “g2_ins” and “g2_out” for service graph 2
Create the functional profile

The functional profile defines the template for any services that are deployed such as L4-L7 device interfaces, IP addresses, rule ID, object addresses, policy rules, source/destination ports, and so on.

Explanation of functional profile objects

Device configuration

The device configuration contains external and internal interfaces that are programmed into the FortiGate VDOM. These are the interfaces (typically external and internal) that are associated to the VDOM. Leave the field in this section untouched for Go-Through mode deployment.

Function configuration

Function configuration consists of:

- **Network**
  - Use this field to configure static routes for IPv4 and IPv6.
- **Policy and objects**
  - This folder is the container for the following folders:
    1. FWServiceFolder – Firewall service object container
    3. IPv4/IPv6 FirewallAddresses – Firewall addresses object container
    4. IPv4 Policy – Firewall policy rule container
    5. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
    6. ScheduleFolder – Schedule container
- **VDOM-folder**
- **VDOM internal and external interfaces**
Create service graph 1

The service graph template is used to tightly couple the functional profile or firewall configuration and combine with the firewall device.

Deploy service graph 1

After the firewall configuration and associated device are combined, you are ready to deploy service graph 1.

On next screen, select the consumer and provider EPGs ("Apps" and "DB") and assign a contract name, or select a predefined contract.
On the next screen, select the logical interfaces ("ins" and "out") defined during the creation of the Layer 4-7 device.

Verify the configuration and then click the Finish.
Create service graph 2
Deploy service graph 2

On next screen, select the consumer and provider EPGs ("Apps2" and "DB2") and assign a contract name, or select a predefined contract.

On the next screen, select the same logical interfaces, "g2_ins" and "g2_out", that were defined during the creation of the Layer 4-7 device.
Verify the configuration and then click Finish.
Verify the creation of device selection policies

Verify the deployment of service graphs
Deploy the firewall device with shared interfaces through multiple service graphs

Prerequisites

- Fabric access policies creation relating to:
- VLAN pools
- Domain
- Attachable access entity profiles
- Interface policies
- Switch policies
- Layer 4-7 device package has imported into Cisco APIC
Basic topology

Workflow

1. Create tenant ("Demo2" in our example)
2. Create VRF ("vrf1" in our example)
3. Create 3 bridge domains ("Web1", "App1", and "DB1" in our example)
4. Associate bridge domains to VRF
5. Create 3 EPGs ("Web1", "App1", and "DB1" in our example)
6. Associate EPGs to bridge domains (EPG "Web1", "App1", and "DB1" are mapped to bridge domain "Web1", "App1", and "DB1" respectively in our example)
7. Create Go-To mode device on Cisco APIC and define 3 logical interfaces
8. Create functional profile
9. Create 2 service graph templates
10. Deploy service graph 2 times on the same device but with different EPG pairs

Configuration
Use case scenarios

Create tenant, VRF and 3 bridge domains on Cisco APIC

Create 3 EPGs
Associate EPG “Web1”, “App1”, and “DB1” to bridge domain “Web1”, “App1”, and “DB1” respectively
Create device with Go-To mode with 3 logical interfaces on Cisco APIC (“Web” “App” and “DB”)

Create the functional profile

The functional profile defines the template for the service(s) that is going to deploy, such as L4-L7 device interface IP addresses, rule ID, object addresses, policy rules, source/destination ports.
Explanation of functional profile objects

Device configuration

Contains external and internal interfaces that will be programmed onto the FortiGate VDOM. These are the interfaces (typically external and internal) that will be associated to the VDOM. Leave the field in this section untouched for Go-Through mode deployment.

Function configurations

Function configuration consists of:

- **Network**
- Use this field to configure static routes for IPv4 and IPv6.
- **Policy and objects**
- This folder is the container for the following folders:
  1. FWServiceFolder – Firewall service object container
  3. IPv4/IPv6 FirewallAddresses – Firewall addresses object container
  4. IPv4 Policy – Firewall policy rule container
  5. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
  6. ScheduleFolder – Schedule container
- **VDOM-folder**
- VDOM internal and external interfaces

You can change of Device Interface name. The default is External/Internal.
In addition, for this use case scenario, App is going to be the shared interface between the two service graphs; therefore, it is crucial that the DeviceInterface name and the content are identical across both service graphs.
Create service graph 1 for Web1 and App1

The service graph template is used to tightly couple the functional profile or firewall configuration and combine with the firewall device.

Deploy service graph 1 Web1 to App1

After you combine the firewall configuration and associated device together, you can deploy service graph 1.
On next screen select the consumer and provider EPGs ("Web1" and "App1") and assign a contract name or select a pre-defined contract.

On the next screen, select the logical interfaces ("app" and "web") defined during the creation of Layer 4-7 device.
Verify the configuration and click FINISH.
Create service graph Graph2 App1 to DB1

On next screen select the consumer and provider EPGs ("App1" and "DB1") and assign a contract name or select a pre-defined contract.
Use case scenarios

On the next screen, select the logical interfaces (App and DB) defined during the creation of Layer 4-7 device.
Confirm the configuration and click FINISH

Verify device selection policies creation
Verify service graphs deployment
Deploy the firewall device in a one-arm configuration with policy based redirect

Prerequisites

- Create fabric access policies relating to:
  - VLAN pools
  - Domain
  - Attachable access entity profiles
  - Interface policies
  - Switch policies
- Import the Layer 4-7 device package into Cisco APIC
- Create a Layer 4-7 policy based redirect (Cisco ACI 2.x above)
- Create dynamic EPG notification (optional)
- Separate the firewall bridge domains. Required for policy based redirect

For N9K93128TX, N9K9396PX, and N9K9396TX switches, the service appliance must not be in the same leaf switch as either the source or destination endpoint group.

Basic Topology

Workflow

1. Create a tenant (“acidemo” in our example)
2. Create a VRF (“acidemo_vrf” in our example)
3. Create 3 bridge domains. In the example they are:
   - “web”
   - “app”
   - “db”
4. Associate bridge domains to VRFs
5. Create 3 EPGs. In the example they are:
   - “web”
   - “app”
   - “db”
6. Associate EPGs to bridge domains
7. Create a dedicated firewall services bridge domain and a subnet on Cisco APIC
8. Create a L4-L7 policy based redirect on Cisco APIC
9. Create a Go-To mode device on Cisco APIC and define 2 logical interfaces
10. Create a functional profile
11. Create a service graph template
12. Deploy the service graph template
Configuration

Create tenant, VRF and 3 bridge domains on Cisco APIC

Add the EPGs default gateway to the bridge domain

In a PBR, the bridge domain becomes the default gateway for the EPGs. You need to assign the gateway address for each EPG that participates in the OneArm BD.

Go to Networking > Bridge Domains > [the target EPG] > Subnets, right-click and click on Create Subnet.
Use the subnet editing window to configure the subnet.

Verify that the subnet has been created.
Repeat for all the EPGs participating in the BD.

Create 3 EPGs

Associate EPGs to bridge domains

- Map EPG “web” to bridge domain “web”
- Map EPG “app” to bridge domain “app”
- Map EPG “db” to bridge domain “db”
Web

FortiGate Connector for Cisco ACI Deployment Package

Fortinet Technologies Inc.
App
Create a dedicated firewall services bridge domain and subnet on Cisco APIC

Uncheck Endpoint Dataplane Learning and create a subnet. This subnet IP will be used later in the default route on the FortiGate.
Create a L4-L7 policy based redirect on Cisco APIC

This IP address will be the same IP address that will be assigned to the FortiGate internal interface. The MAC address is the same as the physical interface MAC on the FortiGate. This can be obtained by using the global CLI command `diagnose hardware deviceinfo nic <port>` on the FortiGate.

Create a device in Go-To mode with 2 logical interfaces on Cisco APIC

You will need to select “internal” and “external” in order to get the configuration to work. However, you will only actually be using the "internal" interface.
Create a functional profile

The functional profile defines the template for any services that are deployed such as L4-L7 device interfaces, IP addresses, rule IDs, object addresses, policy rules, source/destination ports, and so on.

Explanation of functional profile objects

Device configuration

The device configuration contains external and internal interfaces that are programmed into the FortiGate VDOM. These are the interfaces (typically external and internal) that are associated to the VDOM. Delete the external interface as it is not utilized.

Function configuration

The function configuration consists of:

- Network
- This field is use to configure static routes for IPv4 and IPv6.
- Policy and objects

This folder is the container for the following folders:

- FWServiceFolder – Firewall service object container
- IPv4/IPv6 FirewallAddresses – Firewall addresses object container
- IPv4 Policy – Firewall policy rule container
- IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
- ScheduleFolder – Schedule container
- VDOM-folder
- VDOM internal and external interfaces

In this use case, internal is shared for all service graph deployments. The device IP address needs to match the policy based routing destination. Change both of the VDOM interfaces to internal.

A single default route is required and must point to the dedicated firewall services BD subnet's IP address.

Since this is a one-arm configuration, the firewall policies use the same incoming and outgoing interfaces.
Create service graph 1 for Web and App

The service graph template is used to tightly couple the functional profile or firewall configuration, and combine with the firewall device. Check the Route Redirect option box to enable policy based routing.

Deploy service graph 1 Web to App

After you combine the firewall configuration and associated device, you can deploy service graph 1.
On next screen, select the consumer and provider EPGs, “Web” and “App”, then assign a contract name or select a predefined contract. For policy based redirect, the recommend approach is to apply a filter and only redirect applicable traffic.

On the next screen, select the logical interfaces, “app” and “web”, that were defined during the creation of the Layer 4-7 device.
As a workaround to an APIC GUI issue, select what appears to be the incorrect BD causing the SGT to fail to deploy. Select common/default. This will be remedied in the next steps.

Select the device selection policy created by the previous step, consumer connector. Change to the correct BD. In the example it is FwSvc_OneArm. Verify that the cluster interface is set to internal.
Change the provider connector. Change the BD and cluster interface.
Verify the deployment of service graphs
Verify the device deployment

Virtual Device - FGT1500D-1.3-OneArm-acidemo_vrf

The virtual device ID is the same as the VDOM ID which was deployed to the FortiGate. The indicated VLAN is applied to the interface created on the FortiGate under this VDOM for the internal interface.

Verify FortiGate deployment

Verify that the network interface is configured correctly.

Verify that the static route is configured correctly.
Verify that the firewall policy is configured correctly. This policy shows incoming and outgoing traffic on same interface. In this example, no traffic has matched this policy yet.

Verify that the dynamic EPG address group has been updated.

Generate some traffic, such as Ping queries, to verify connectivity.
Check to see if the counters have increased.

Service chaining

For this use case, we are leveraging one FortiGate and one ADC devices. In this service chaining topology, incoming client traffic can be load-balanced by the ADC to the FortiGate in the back. The FortiGate operates in two-arm mode while the ADC operates in one-arm mode. Policy based routing is enforced on the FortiGate.

Topology
Firmware required

The following firmware and models are used:

- Cisco ACI: 3.1(2.o)
- FortiGate (3700D): 5.6.4
- FortiADC (2000D): 5.0.1

Prerequisites

Before you can replicate the use case, create the following items:

- Tenant: Demo1
- VRF: VRF1
- BDs:
  - Client (Client BD)
  - Server (Server BD)
  - FW_Ext (Firewall External Interface BD)
  - FW_Int (Firewall Internal Interface BD)
  - LB (Load Balancer BD)
- EPGs:
  - ADCClient
  - ADCServer

Workflow

The process to set up service chaining is as follows:

- Create L4-L7 devices with Go-To mode on Cisco ACI
- Create functional profiles for FortiADC and FortiGate
- Create service graph template
- Deploy service graph

Create L4-L7 devices Go-To mode on Cisco ACI

FortiGate

Configuration pane for FortiGate
Use case scenarios

FortiADC

Configuration pane for FortiADC

Create functional profiles for FortiADC and FortiGate

Functional profiles
Create a service graph template

Tenant

Create policy based redirects (PBR) policies

PBRs
Deploy a service graph

Apply L4-L7 service graph template to endpoint groups (EPGs) - Step #1

Apply L4-L7 service graph template to EPGs - Step #2
Apply L4-L7 service graph template to EPGs - Step #3

STEP 3 > FGT15248 Configuration
config parameters for the selected device

Apply L4-L7 service graph template to EPGs - Step #4
Use case scenarios

STEP 4 > ADC2K Configuration
config parameters for the selected device

Profile Name:
Features

Required Parameters  All Parameters

<table>
<thead>
<tr>
<th>Folder/Parameter</th>
<th>Name</th>
<th>Value</th>
<th>Apply to specific device</th>
<th>Write Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Config</td>
<td>Device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; Device Interface</td>
<td>internal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function Config</td>
<td>Function</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; LoadBalance Objects</td>
<td>LB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; Mode</td>
<td>mode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; Network</td>
<td>Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; VDOM-Folder</td>
<td>vdom-folder</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Deploy service graph

After the graph is deployed, the status and configuration should appear as follows:

The contract

The FortiADC virtual device
The FortiGate virtual device
FortiGate configurations

Interfaces on FortiGate

Static routes on FortiGate
Use case scenarios

IPv4 policies on FortiGate

FortiADC configurations

Interfaces

Routing
Use case scenarios

Virtual Server (Basic section)

Virtual Server (General section)
Use case scenarios

Virtual Server (NAT Source Pool tab)

Real Server Pool (Real Server Pool tab)

Real Server Pool (Real Server tab)

All Sessions (Session Table tab)
Use case scenarios

FortiGate Connector for Cisco ACI Deployment Package

Fortinet Technologies Inc.