cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Firepower Threat Defense Virtual Routing and Forwarding (VRF)

Luis Silva Benavides – Customer Success Specialist
@LuisSilva_1990

BRKSEC-3580

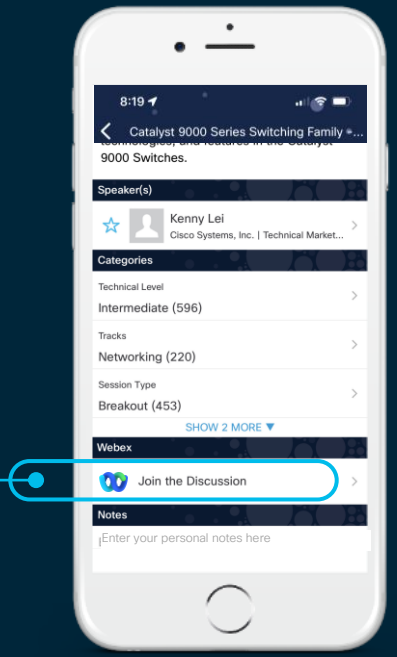
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3580

Webex spaces will be moderated by the speaker until June 17, 2022.

About your Speaker

Customer Success Specialist

- Costa Rica / Texas
- 13+ years of experience
- TAC, Advanced Services, CSS
- CCIE Security / CISSP®

Agenda

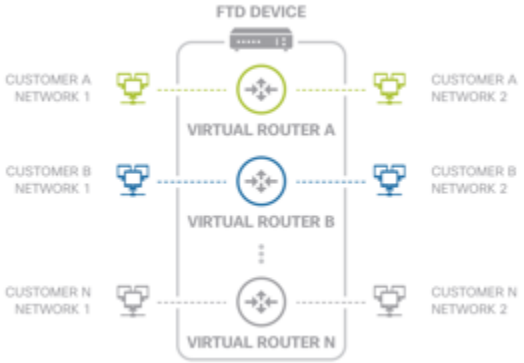
- Introduction
- Virtual Routing and Forwarding
- Configuring VRF
- Configuring Routing Protocols
- Troubleshooting VRF
- Conclusion

Introduction

Virtual Routing and Forwarding

Why Virtual Routers/Routing?

- Separate Routing/Forwarding tables
- VRF-Lite
- Overlapping IP address
- Multi-Virtual Router Support (FXOS + VRF =Multi-Context use cases)



Advantages (FTD Version 6.6+)

- Routing segregation on FTD
- Overlapping IP address on FTD interfaces
- Connection events (ingress/egress virtual router)

Access Control Policy	Access Control Rule	Network Analysis Policy	Prefilter Policy	Tunnel/Prefilter Rule	Source SGT	Destination SGT	Endpoint Profile	Endpoint Location	Device	Ingress Interface	Egress Interface	Ingress Virtual Router	Egress Virtual Router
ACP_CL	Eng_to_Sales	Balanced Security and Connectivity	Default Prefilter Policy						FTD 6.7	Engineering	Sales	VRF_Engineering	VRF_Sales

VRF Support

Device	Maximum Virtual Routers	
ASA	10-20	
Firepower 1000*	5-10	*1010 (7.2+)
Firepower 2100	10-40	
Firepower 3100	15-100	
Firepower 4100	60-100	
Firepower 9300	60-100	
Virtual FTD	30	
ISA 3000	10 (7.0+)	

Configuration Guide

No License required

Routing Policies

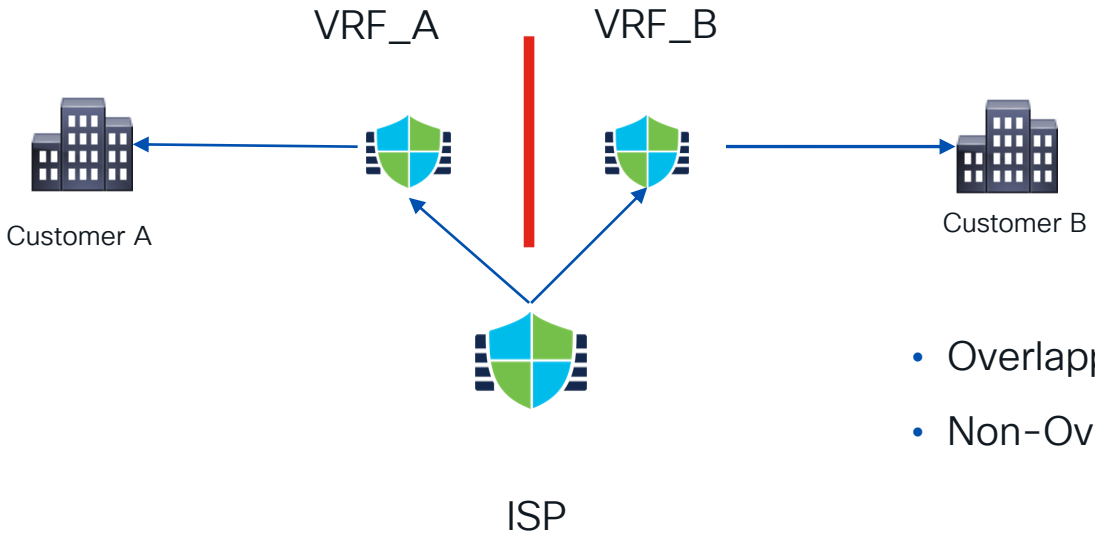
Policies	Global VRF	User VRF
Static Route	✓	✓
OSPFv2	✓	✓
OSPFv3	✓	X
RIP	✓	X
BGPv4	✓	✓
BGPv6	✓	✓ (7.1+)
IRB (BVI)	✓	✓
EIGRP	✓	X

Overlapping Networks – Feature Support

Policies	Non-Overlapping	Overlapping Networks
Routing & IRB	✓	✓
AVC	✓	✓
SSL Decryption	✓	✓
Intrusion and Malware Detection (IPS and File Policy)	✓	✓
VPN	✓	✓
Malware Event Analysis (Host Profiles, IoC, File Trajectory)	✓	X
Threat Intelligence (TID)	✓	X

Use case #1 – Service Provider

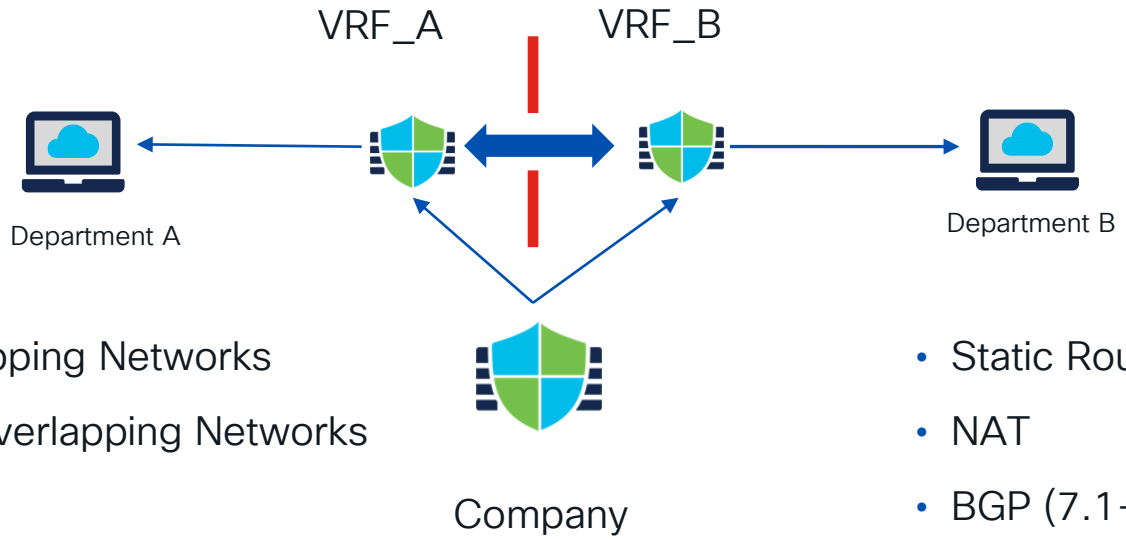
- Separate routing tables



- Overlapping Networks
- Non-Overlapping Networks

Use case #2 – Enterprise

- Connectivity between VRFs (Route Leaking)

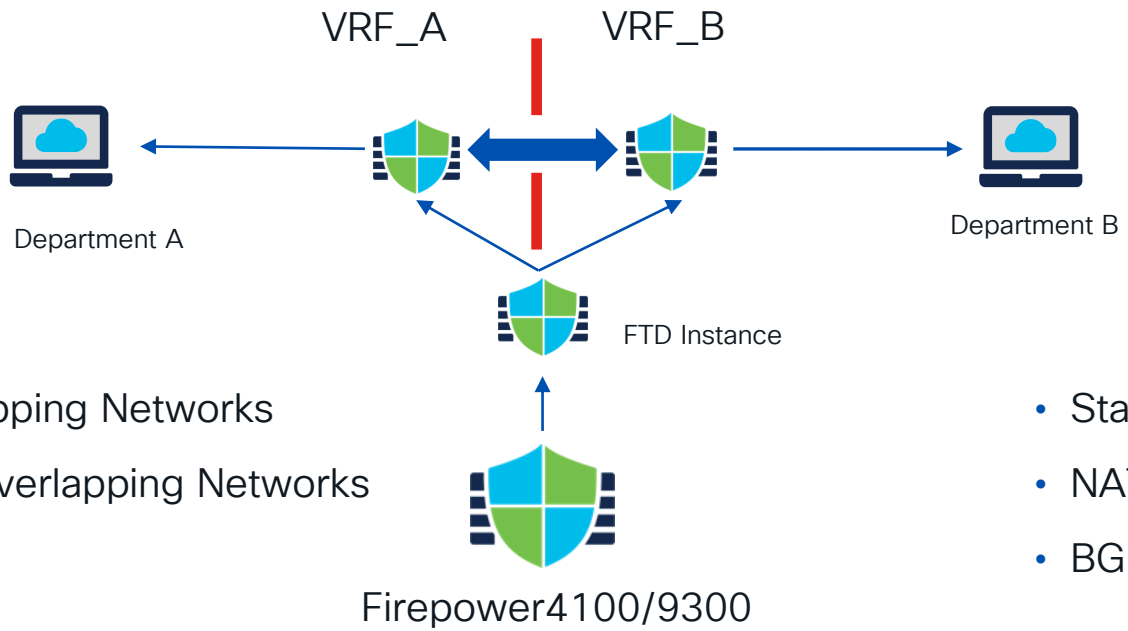


- Overlapping Networks
- Non-Overlapping Networks

- Static Routes
- NAT
- BGP (7.1+)

Use case #3 – Multi-Instance and VRF

- Connectivity between VRFs in a Multi-Instance Environment



- Overlapping Networks
- Non-Overlapping Networks

- Static Routes
- NAT
- BGP (7.1+)

Configuring VRF

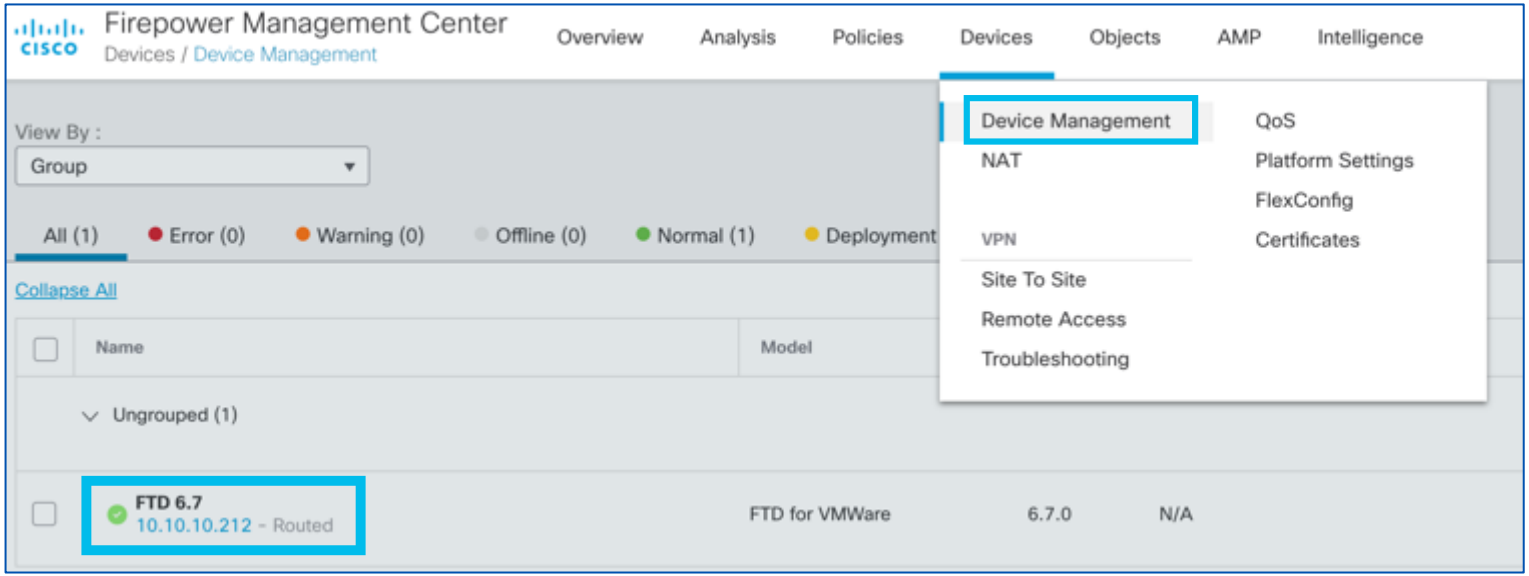
Demo 1: VRF configuration on FMC

VRF configuration on FMC

Subtitle

For your reference

- Device > Device Management > FTD



VRF configuration on FMC

Subtitle

For your reference

- Routing > Manage Virtual Routers > Add Virtual Router

FTD 6.7

Cisco Firepower Threat Defense for VMWare

Save Cancel

Device Routing Interfaces Inline Sets DHCP

Manage Virtual Routers

Select

Virtual Routers

Virtual routing and forwarding (VRF) is a technology included in IP (Internet Protocol) network routers that allows multiple instances of a routing table to exist in a router and work simultaneously. This increases functionality by allowing network paths to be segmented without using multiple devices.

Total Virtual Router Configured : (1)

Search Virtual Router or Interface

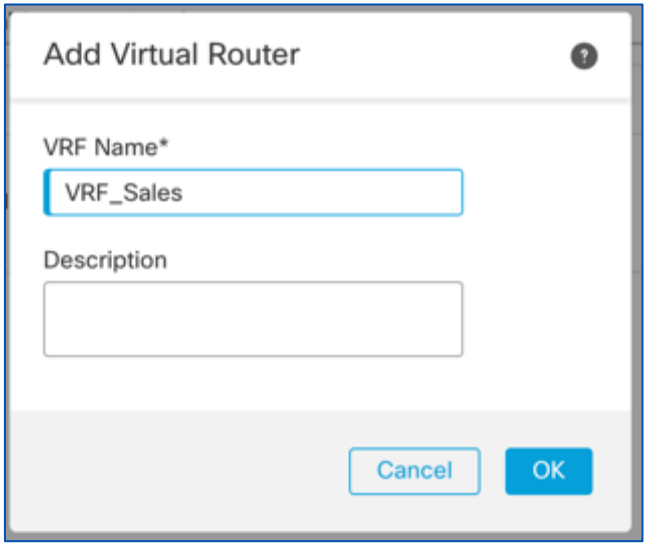
+ Add Virtual Router

Virtual Router	Interfaces	Show/TroubleShoot
Global	diagnostic, Outside, Inside	>_ Routes >_ IPv6 Routes >_ BGP Summary >_ OSPF Summary

VRF configuration on FMC

For your reference

- Add a new Virtual Router



VRF configuration on FMC

For your reference

- Assign interfaces to VRF

FTD 6.7

Cisco Firepower Threat Defense for VMWare

You have unsaved changes Save

Device Routing Interfaces Inline Sets DHCP

Manage Virtual Routers

VRF_Sales

Virtual Router Properties

OSPF

BGP

IPv4

Static Route

General Settings

BGP

Virtual Router Properties

These are the basic details of this virtual router.

VRF Name:

VRF_Sales

Description:

Select Interface:

Search

Available Interfaces

Outside

Inside

Sales

Engineering

Add

Selected Interfaces

Sales

VRF configuration on FMC

For your reference

- Verify VRF assignment under “Interfaces”

FTD 6.7

Cisco Firepower Threat Defense for VMWare

Device | Routing | Interfaces | Inline Sets | DHCP

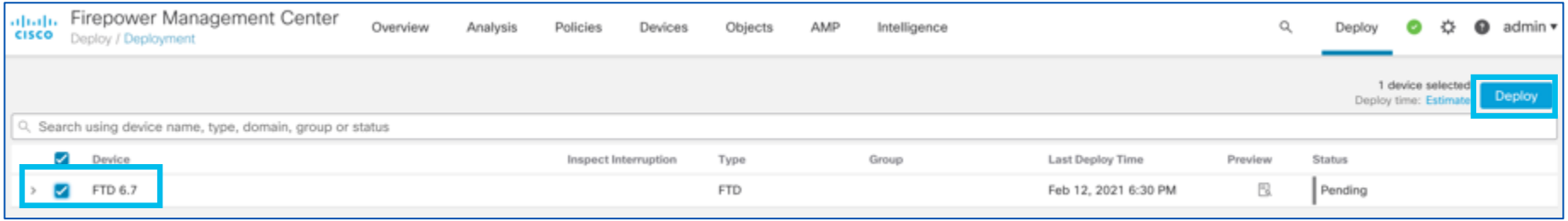
Search by name | Sync Device | Ad

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Virtual Router
Diagnostic0/0	diagnostic	Physical				Global
GigabitEthernet0/0	Outside	Physical	Out_zone		10.10.10.213/24(Static)	Global
GigabitEthernet0/1	Inside	Physical	In_zone		192.168.50.1/24(Static)	Global
GigabitEthernet0/2	Sales	Physical	Sales_Zone		172.16.1.1/24(Static)	VRF_Sales
GigabitEthernet0/3	Engineering	Physical	Eng_zone		172.16.2.1/24(Static)	VRF_Engineering

VRF configuration on FMC

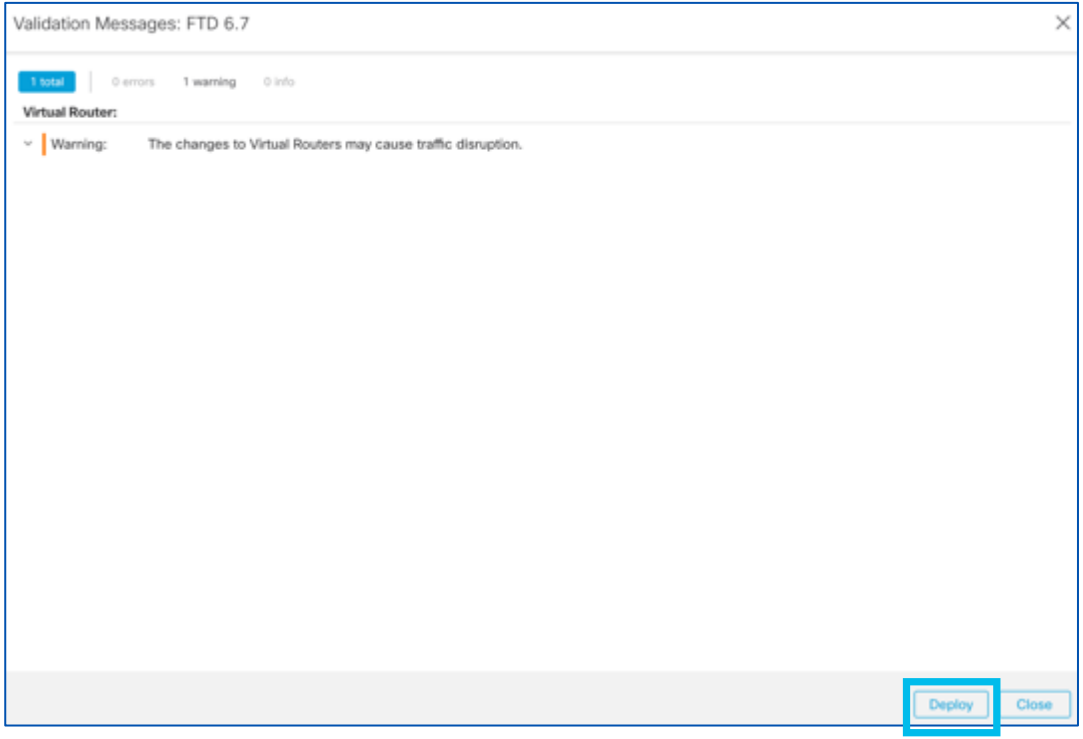
For your reference

- Deploy changes



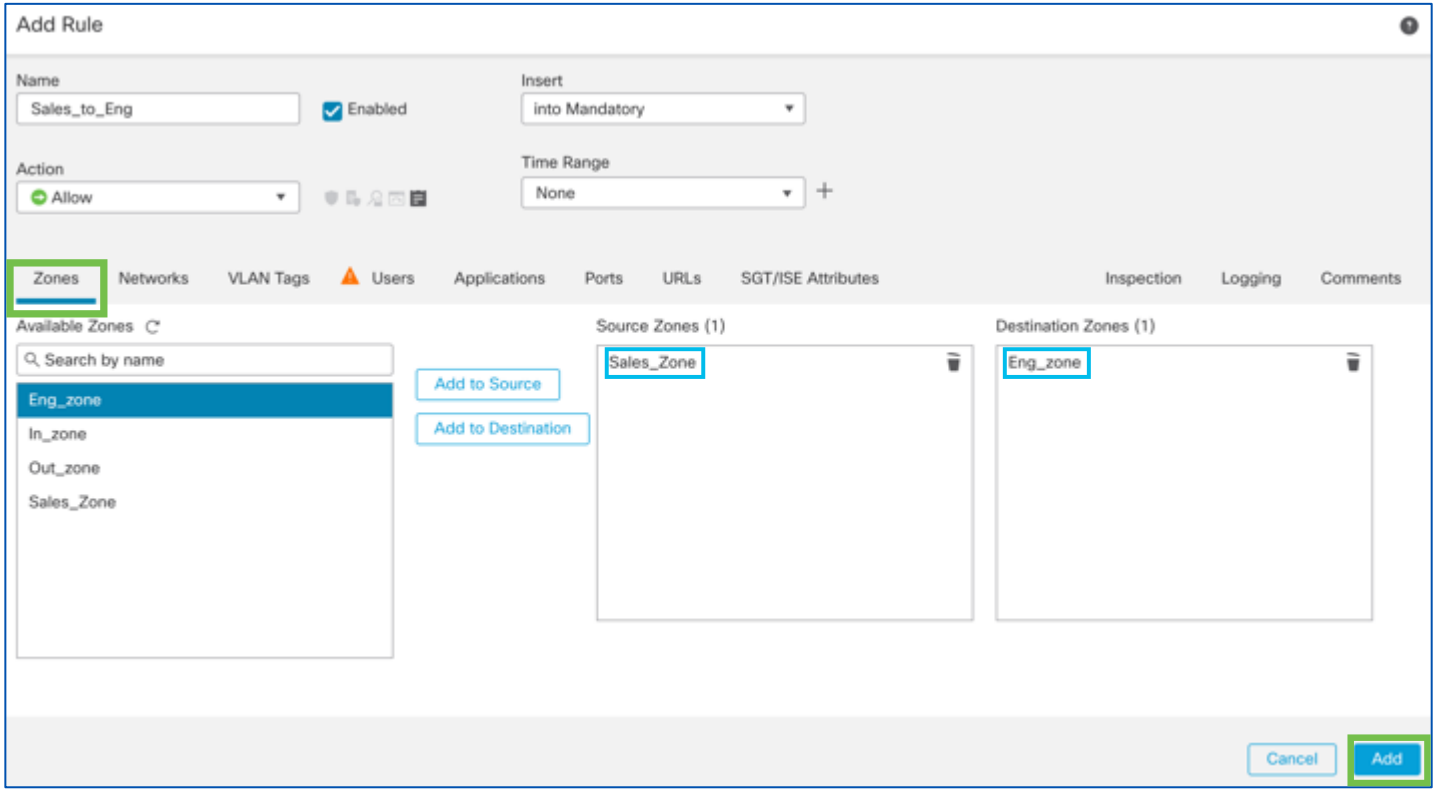
VRF configuration on FMC

- Deploy changes



Access Control Policy VRF- Aware

For your reference



Access Control Policy VRF- Aware

For your reference

Add Rule

Name: Sales_to_Eng

Enabled

Insert: into Mandatory

Action: Allow

Time Range: None

Zones | Networks | VLAN Tags | Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Available Networks

Search by name or value

Networks | Geolocation

any-ipv4
any-ipv6
Eng_Network
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8
IPv4-Private-172.16.0.0-12

Add To Source Networks

Add to Destination

Source Networks (1)

Source | Original Client

Sales_Net

Enter an IP address | Add

Destination Networks (1)

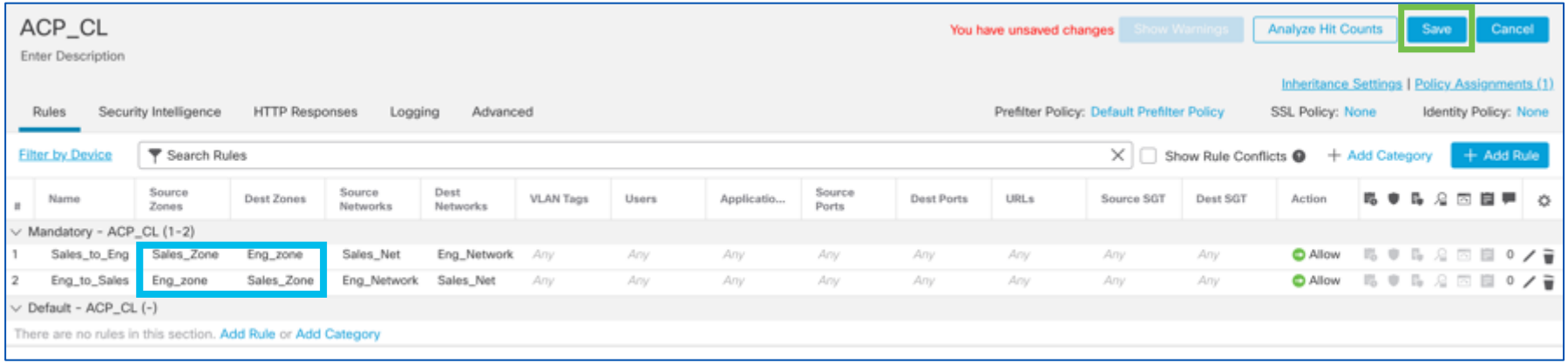
Eng_Network

Enter an IP address | Add

Cancel | Add

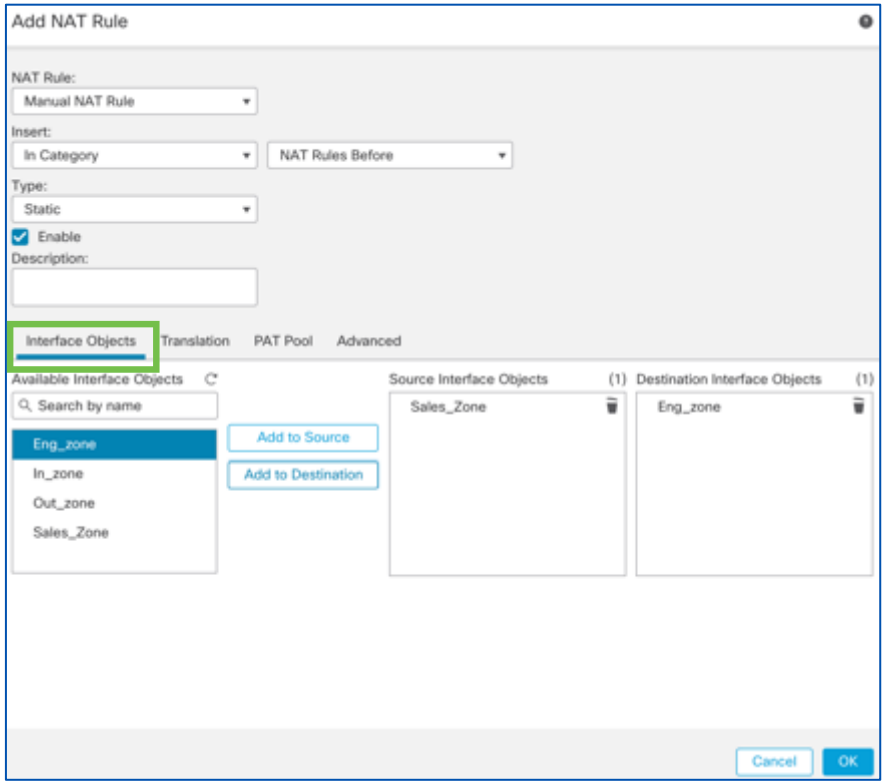
Access Control Policy VRF- Aware

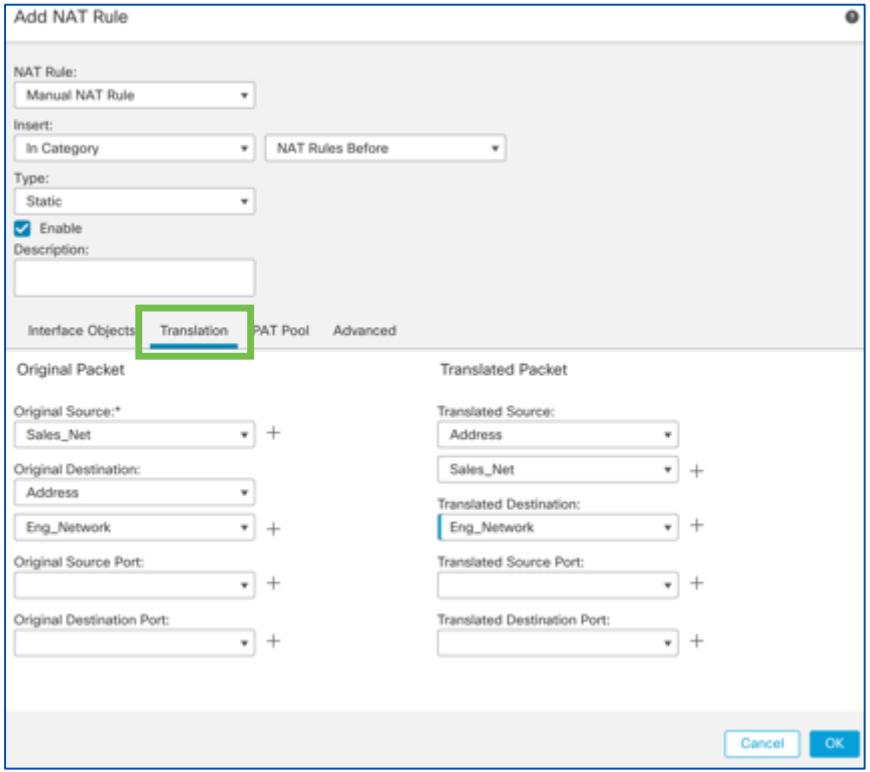
For your reference



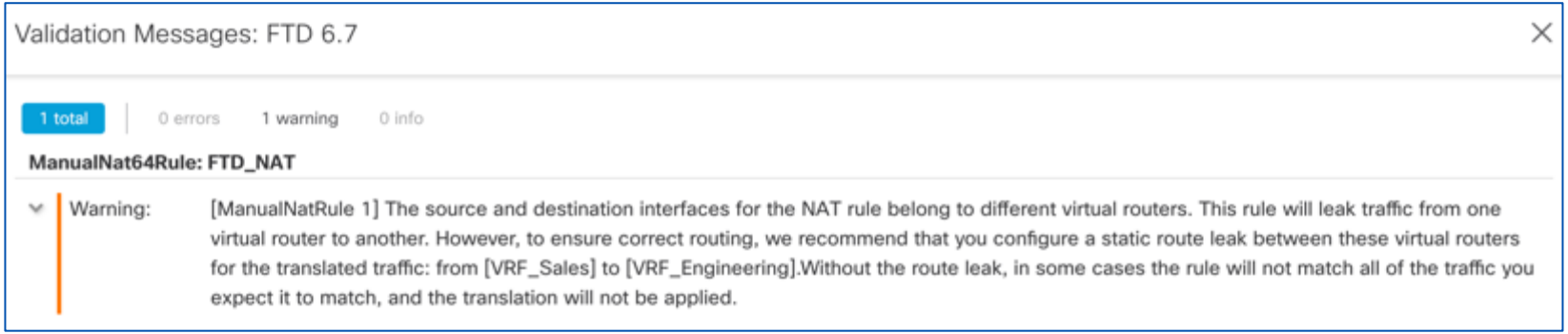
NAT Policy VRF- Aware

For your reference



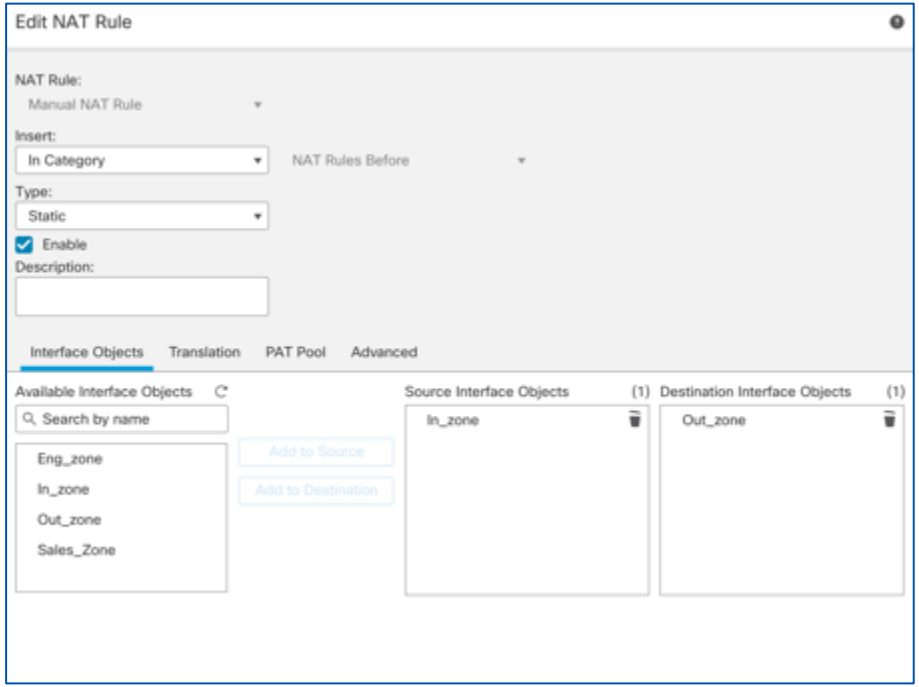


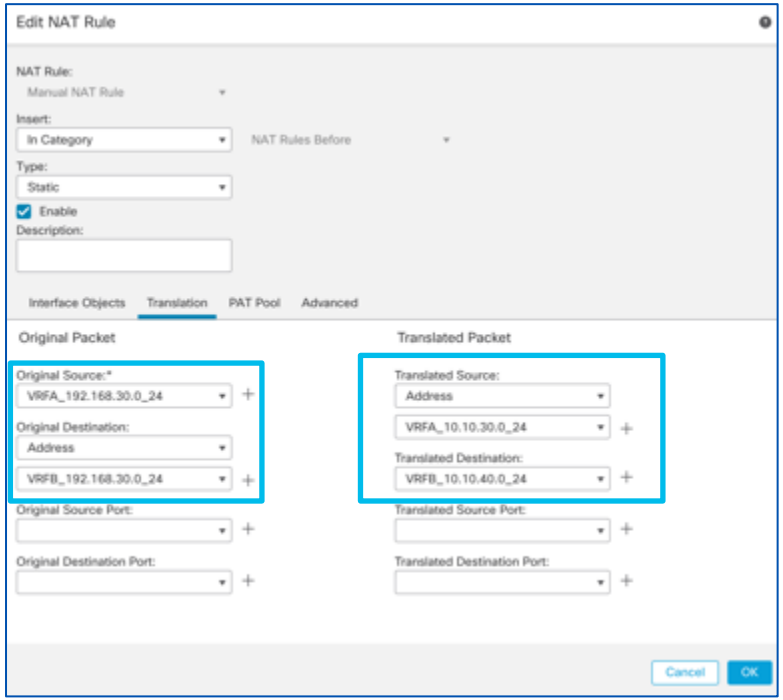
NAT Policy VRF- Aware



NAT Policy VRF- Aware – Overlapping Networks

For your reference



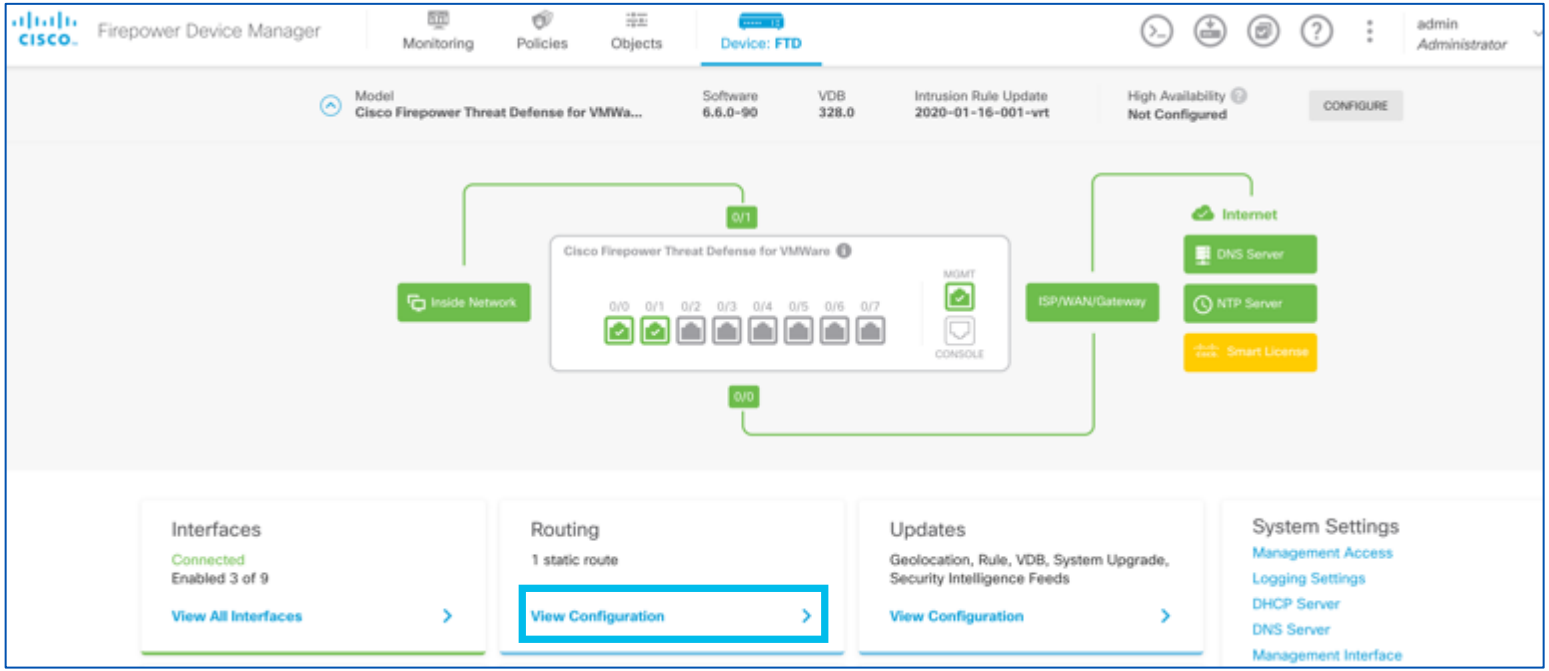


Demo 2: Configuring VRF on FDM

VRF configuration on FDM

For your reference

- Routing > View Configuration

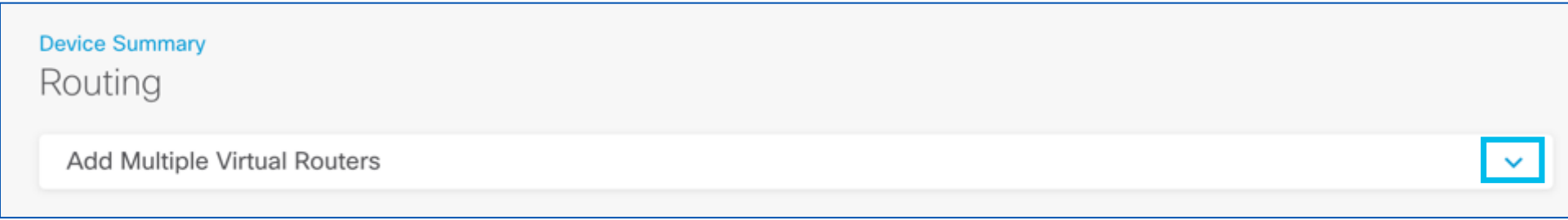


VRF configuration on FDM

Subtitle

For your reference

- Routing > Add Multiple Virtual Routers



VRF configuration on FDM

For your reference

- Create First Custom Virtual Router

Device Summary

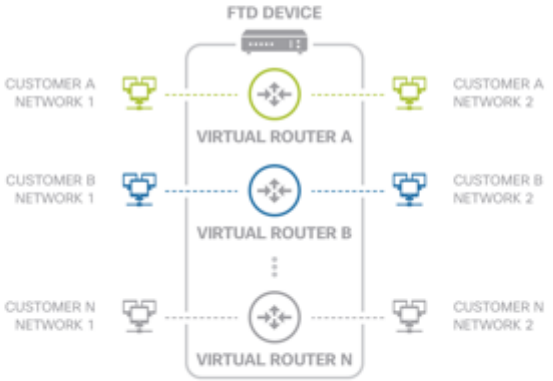
Routing

Virtual Route Forwarding (Virtual Routing) Description

You can create multiple virtual routing and forwarding instances, called virtual routers, to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device.
Thus, you can provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general-purpose corporate network.

How Multiple Virtual Routers Work

Multiple Virtual Router mode is enabled automatically if there is at least one custom Virtual Router.

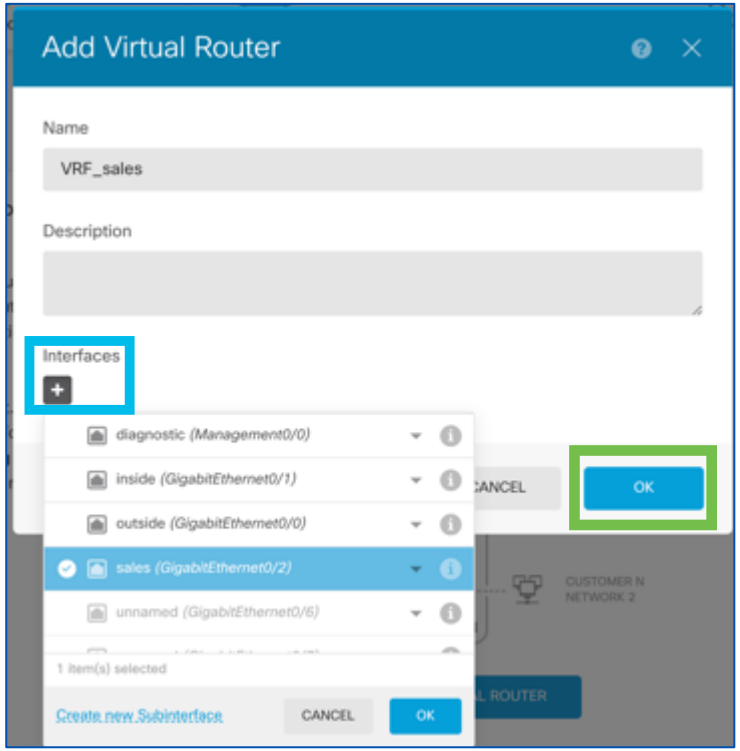


CREATE FIRST CUSTOM VIRTUAL ROUTER

VRF configuration on FDM

For your reference

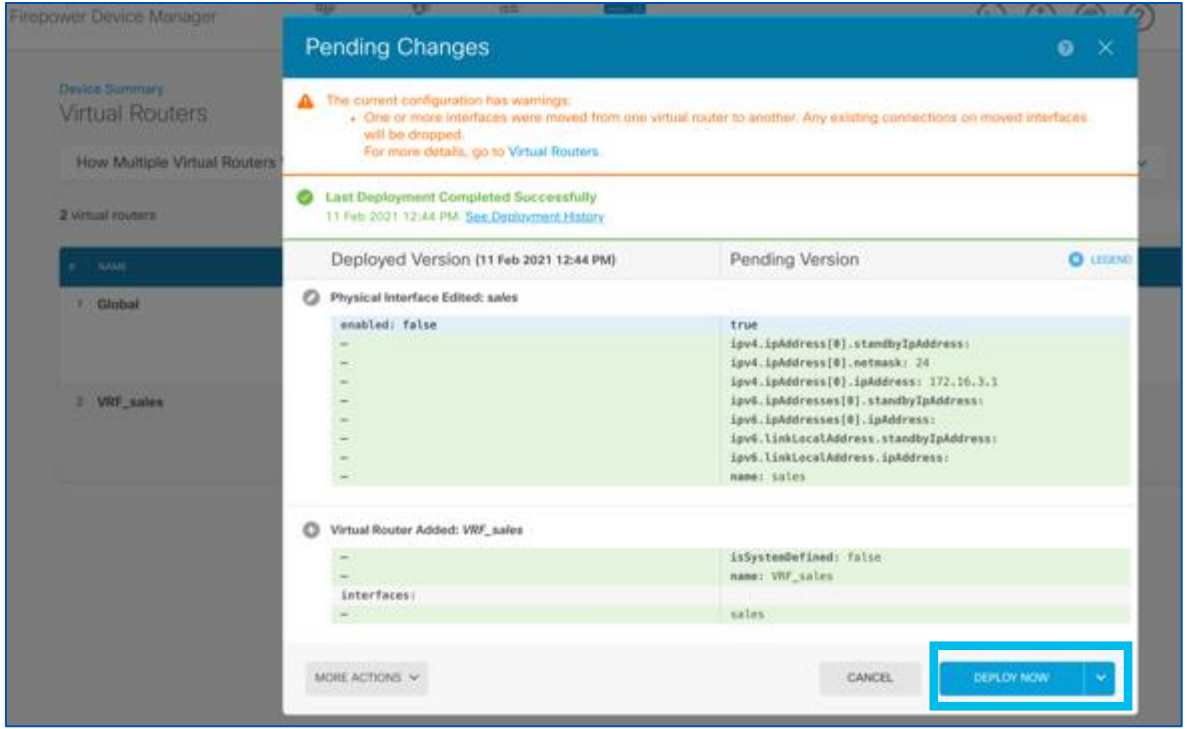
- Add a new Virtual Router and assign interfaces



VRF configuration on FDM

For your reference

- Deploy changes



VRF configuration on FDM

For your reference

- Verified deployed changes

Device Summary

Virtual Routers

How Multiple Virtual Routers Work

BGP Global Settings

2 virtual routers

Search

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	diagnostic inside outside	Routes Ipv6 routes BGP OSPF	
2	VRF_sales	sales	Routes Ipv6 routes BGP OSPF	

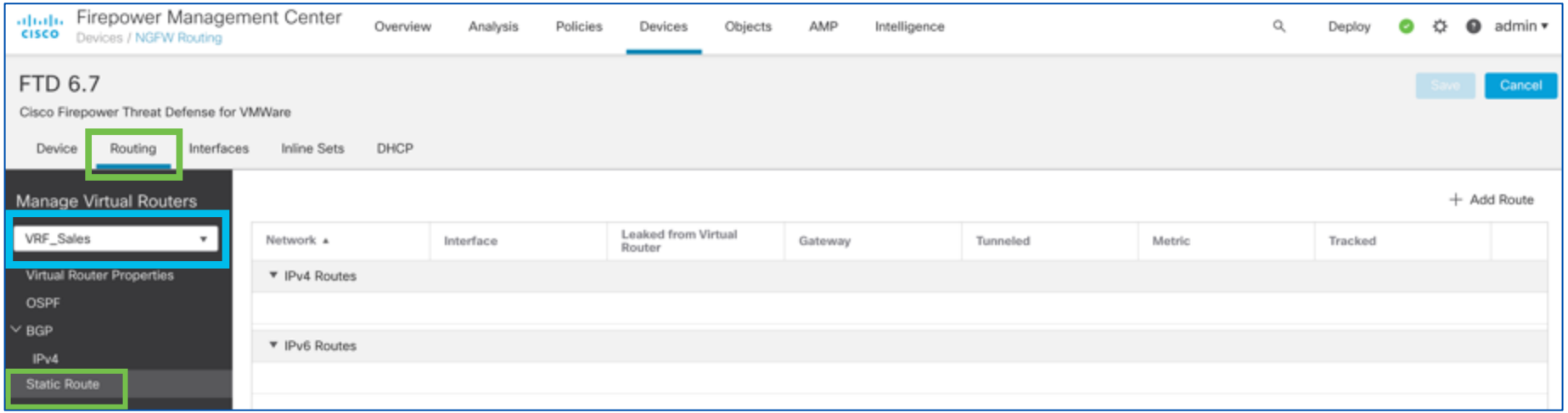
Configuring Routing Protocols

Demo 3: Configuring Static Routing on FMC

Static Routing on FMC

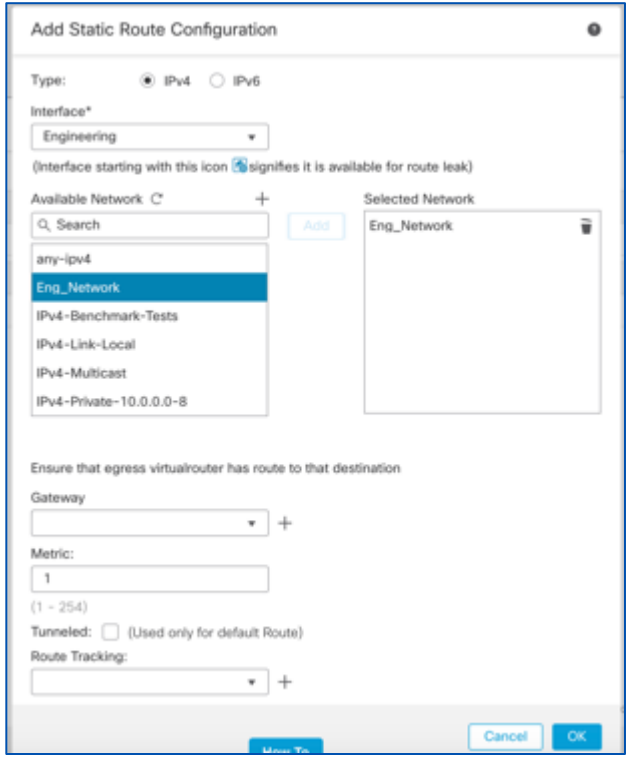
For your reference

- Routing > Desired VRF > Static Route



Static Routing on FMC

For your reference



Static Routing on FMC

For your reference

- Save > Deploy Changes

FTD 6.7

Cisco Firepower Threat Defense for VMWare

You have unsaved changes | Save | Cancel

Device | Routing | Interfaces | Inline Sets | DHCP

Manage Virtual Routers

VRF_Sales

Virtual Router Properties

OSPF

✓ BGP

IPv4

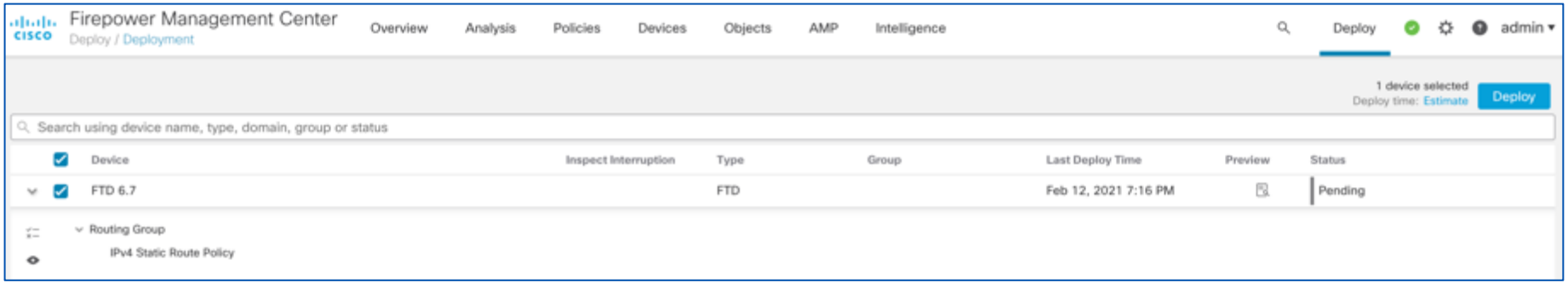
+ Add Route

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
Eng_Network	Engineering	VRF_Engineering		false	1	
▼ IPv6 Routes						

Static Routing on FMC

For your reference

- Deploy > Deploy Changes



Static Routing on FMC – Verify Configuration

For your reference

- VRF_Sales > _Routes

Firepower Management Center
Devices / NGFW Routing

Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence | Deploy | admin

FTD 6.7
Cisco Firepower Threat Defense for VMWare

Device | Routing | Interfaces | Inline Sets | DHCP

Save | Cancel

Manage Virtual Routers
Select

Virtual Routers

Virtual routing and forwarding functionality by allowing netw

nstances of a routing table to exist in a router and work simultaneously. This increases

Total Virtual Router Configure

+ Add Virtual Router

show route vrf VRF_Sales

```
> show route vrf VRF_Sales

Routing Table: VRF_Sales
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
Gateway of last resort is not set

C 172.16.1.0 255.255.255.0 is directly connected, Sales
L 172.16.1.1 255.255.255.255 is directly connected, Sales
SI 172.16.2.0 255.255.255.0 [1/0] is directly connected, Engineering
```

Virtual Router		Show/TroubleShoot
Global		>_ Routes >_ IPv6 Routes >_ BGP Summary >_ OSPF Summary
VRF_Engineering	Engineering	>_ Routes >_ IPv6 Routes >_ BGP Summary >_ OSPF Summary
VRF_Sales	Sales	>_ Routes >_ IPv6 Routes >_ BGP Summary >_ OSPF Summary

Demo 4 : Configuring BGP on FMC

Border Gateway Protocol (BGP) on FMC

For your reference

- Routing > General Settings> BGP

FTD 6.7

Cisco Firepower Threat Defense for VMWare

You have unsaved changes Save Cancel

Device Routing Interfaces Inline Sets DHCP

Manage Virtual Routers

Global

Virtual Router Properties
OSPF
OSPFv3
RIP
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM
Multicast Routes
Multicast Boundary Filter

General Settings
BGP

Enable BGP:

AS Number*

Override BGP general settings router-id address:

Router Id

Automatic

IP Address*

General	
Scanning Interval	60
Number of AS numbers in AS_PATH attribute of received routes	None
Log Neighbor Changes	Yes
Use TCP path MTU discovery	Yes
Reset session upon failover	Yes
Enforce the first AS is peer's AS for EBGP routes	Yes
Use dot notation for AS number	No
Aggregate Timer	30

Best Path Selection

Neighbor Timers	
Keepalive Interval	60
Hold time	180
Min hold time	0

Next Hop	
Address tracking	Yes
Delay interval	5

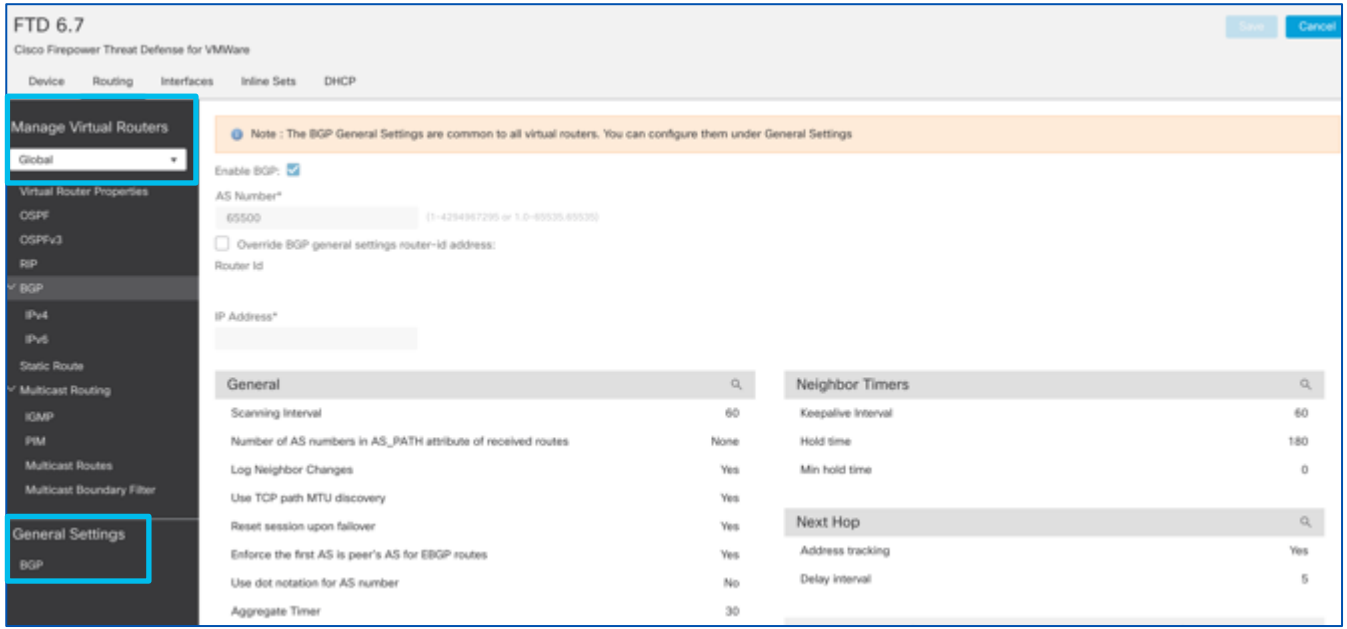
Graceful Restart (use in failover or spanned cluster mode)

Graceful Restart No

Border Gateway Protocol (BGP) on FMC

For your reference

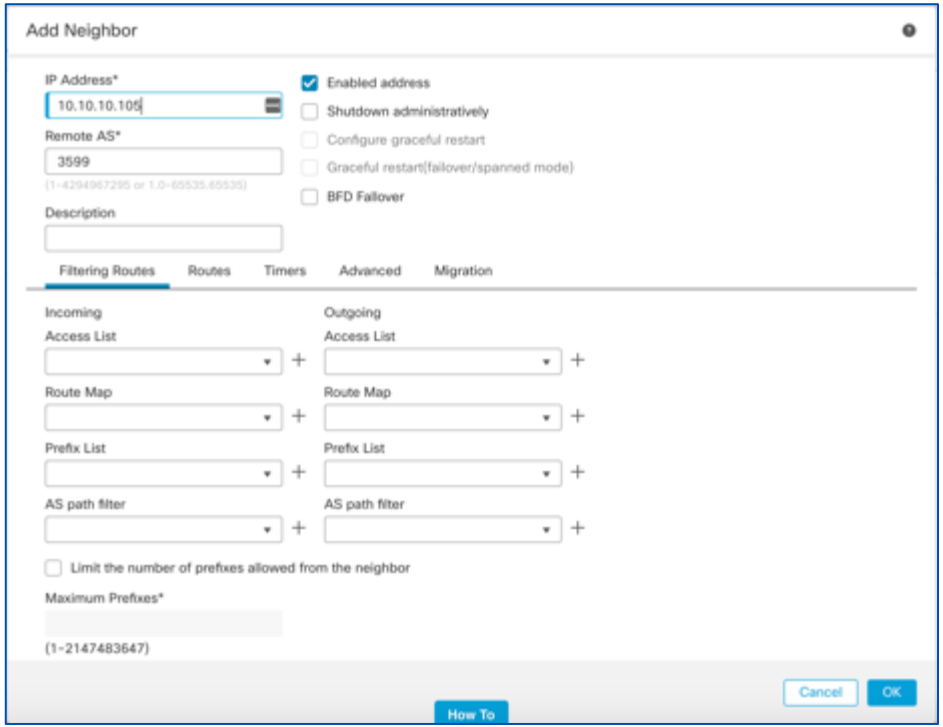
- Routing > Desired VRF> BGP > IPv4



Border Gateway Protocol (BGP) on FMC

For your reference

- Routing > Desired VRF> BGP > IPv4 > Neighbor



Border Gateway Protocol (BGP) on FMC

For your reference

- Routing > Manage Virtual Routers> Desired VRF > Route | BGP Summary

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
Gateway of last resort is not set

C 10.10.10.0 255.255.255.0 is directly connected, Outside
L 10.10.10.213 255.255.255.255 is directly connected, Outside
B 10.255.254.255 255.255.255.255 [20/0] via 10.10.10.32, 00:03:11
B 10.255.255.255 255.255.255.255 [20/0] via 10.10.10.32, 00:03:11
C 192.168.50.0 255.255.255.0 is directly connected, Inside
L 192.168.50.1 255.255.255.255 is directly connected, Inside
```

show bgp summary

```
> show bgp summary
BGP router identifier 192.168.50.1, local AS number 65500
BGP table version is 3, main routing table version 3
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 792 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.32 4 65536 10 9 3 0 0 00:05:46 2
10.10.10.105 4 3599 0 0 1 0 0 never Active
```

Demo 5: Configuring OSPF on FMC

OSFP on FMC

For your reference

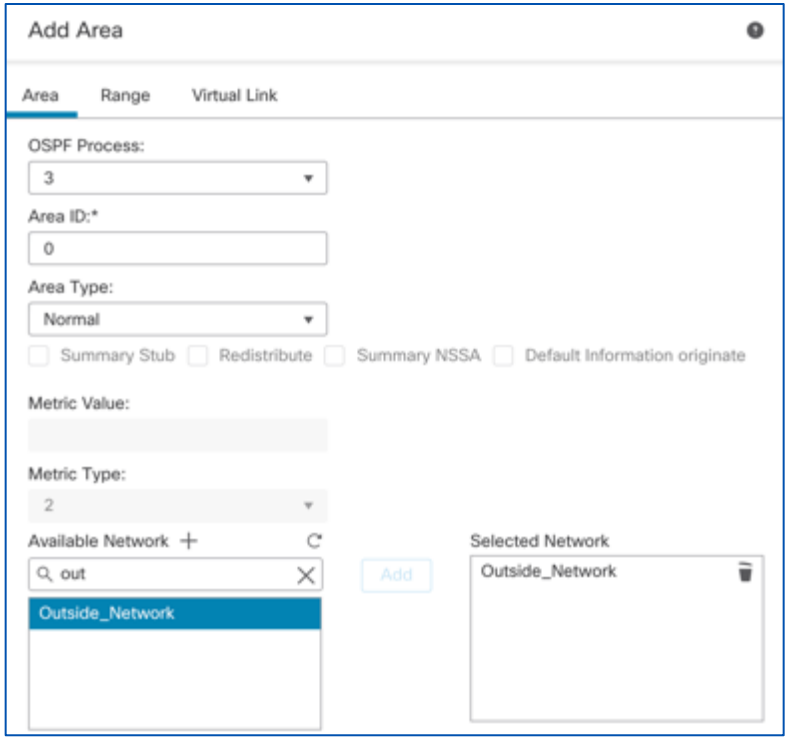
- Routing > Desired VRF> OSPF

FTD 6.7
Cisco Firepower Threat Defense for VMWare
You have unsaved changes Save Cancel
Device Routing Interfaces Inline Sets DHCP
Manage Virtual Routers
VRF_Sales
Virtual Router Properties
OSPF
BGP
IPv4
Static Route
General Settings
BGP
Process 1 ID: 3
OSPF Role:
Internal Router
Enter Description here
Advanced
Process 2 ID:
OSPF Role:
Internal Router
Enter Description here
Advanced
Area Redistribution InterArea Filter Rule Summary Address Interface
+ Add
OSPF Process | Area ID | Area Type | Networks | Options | Authentication | Cost | Range | Virtual-Link
No records to display

OSFP on FMC

For your reference

- Add a Neighbor



OSFP on FMC

For your reference

- Save and deploy changes

FTD 6.7
Cisco Firepower Threat Defense for VMWare
You have unsaved changes | Save | Cancel

Device | Routing | Interfaces | Inline Sets | DHCP

Manage Virtual Routers
VRF_Sales
Virtual Router Properties
OSPF
BGP
IPv4
Static Route
General Settings
BGP

Process 1 ID: 3
OSPF Role:
Internal Router | Enter Description here | Advanced
Process 2 ID:
OSPF Role:
Internal Router | Enter Description here | Advanced

Area | Redistribution | InterArea | Filter Rule | Summary Address | Interface

+ Add

OSPF Process	Area ID	Area Type	Networks	Options	Authentication	Cost	Range	Virtual-Link
3	0	normal	Outside_Network	false	none			

OSFP on FMC

For your reference

- Routing > Manage Virtual Routers > route | OSPF Summary

show route vrf VRF_Sales

```
> show route vrf VRF_Sales


Routing Table: VRF_Sales
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
Gateway of last resort is 10.10.10.1 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.10.10.1, Outside
C 10.10.10.0 255.255.255.0 is directly connected, Outside
L 10.10.10.213 255.255.255.255 is directly connected, Outside
B 10.255.254.255 255.255.255.255 [20/0] via 10.10.10.32, 00:13:21
B 10.255.255.255 255.255.255.255 [20/0] via 10.10.10.32, 00:13:21
C 172.16.1.0 255.255.255.0 is directly connected, Sales
L 172.16.1.1 255.255.255.255 is directly connected, Sales
SI 172.16.2.0 255.255.255.0 [1/0] is directly connected, Engineering
O E2 192.168.30.0 255.255.255.0
[110/20] via 10.10.10.30, 00:01:37, Outside
```

show ospf vrf VRF_Sales

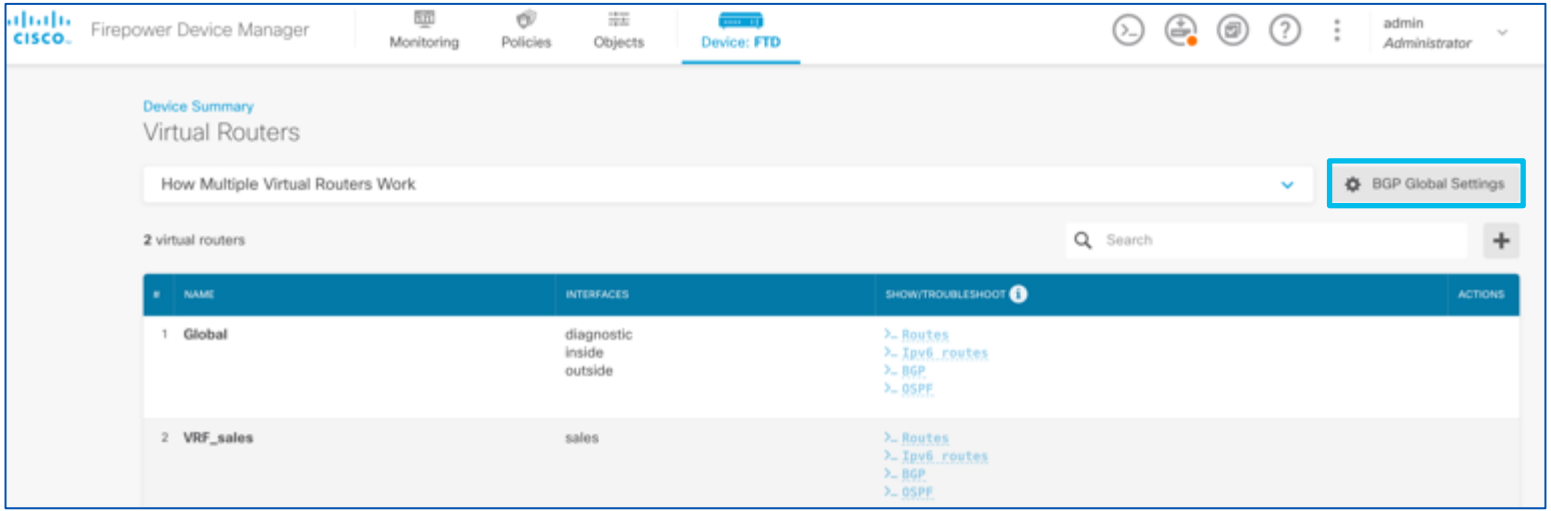
```
> show ospf vrf VRF_Sales

Routing Process "ospf 3" with ID 172.16.1.1 and vrf VRF_Sales
Start time: 2d02h, Time elapsed: 00:02:34.240
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 1. Checksum Sum 0x23c2
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
```

Demo 6: Configuring BGP on FDM

Border Gateway Protocol (BGP) on FDM

For your reference

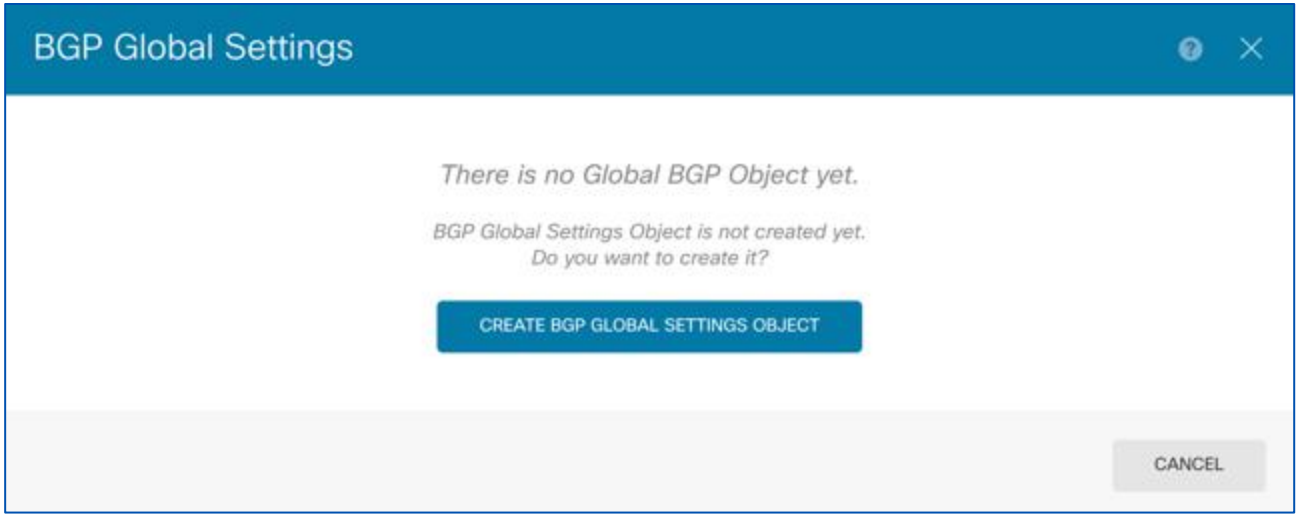
- Routing > BGP General Settings



Border Gateway Protocol (BGP) on FDM

For your reference

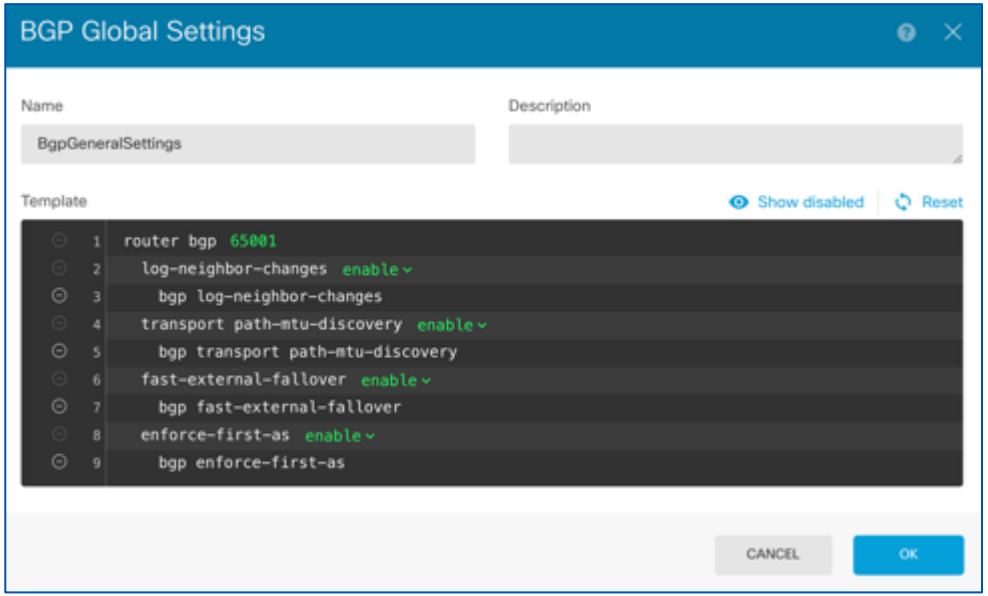
- Create BGP General Settings Object



Border Gateway Protocol (BGP) on FDM

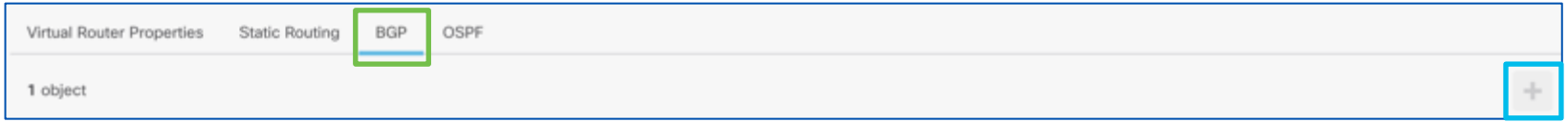
For your reference

- BGP General Settings



Border Gateway Protocol (BGP) on FDM

For your reference

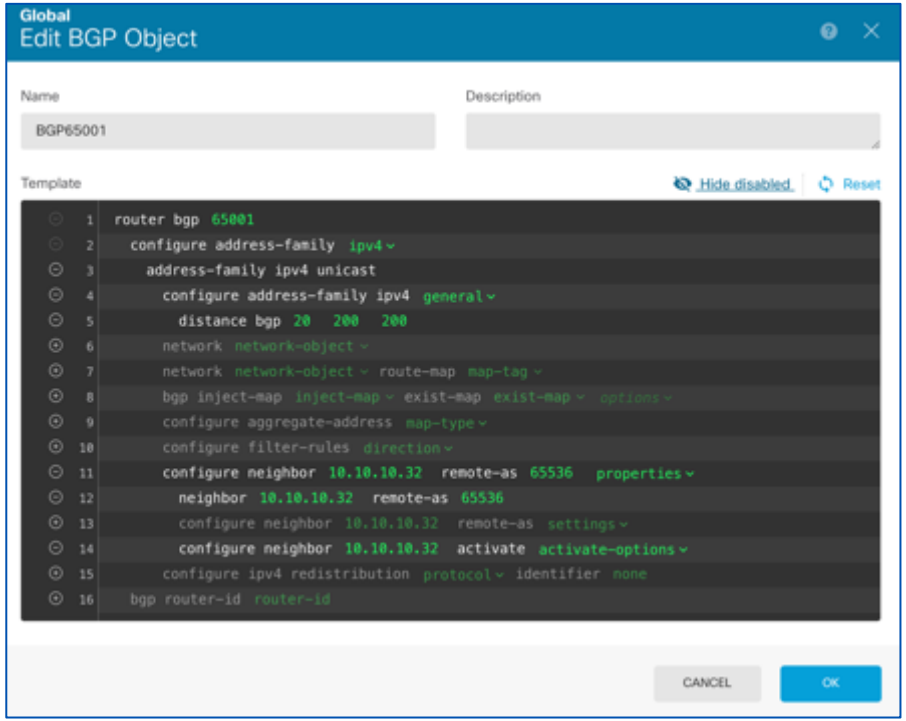


Border Gateway Protocol (BGP) on FDM

BGP Object

For your reference

- Save and Deploy changes



Border Gateway Protocol (BGP) on FDM

For your reference

- Verify routing table and BGP neighbor

CLI Console

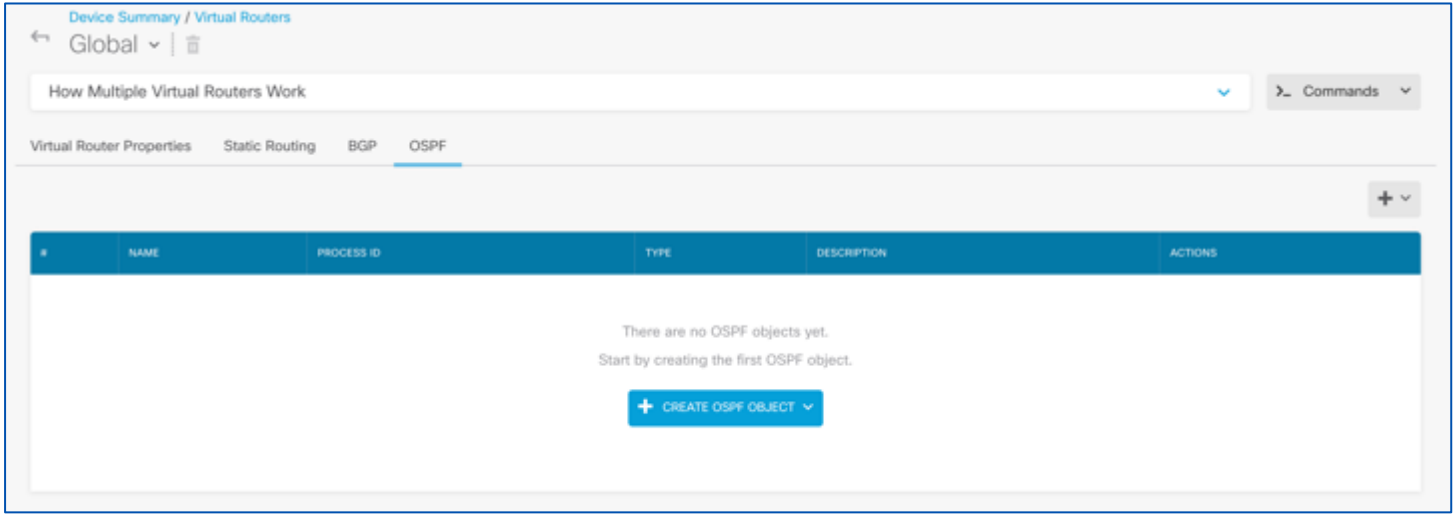
```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.10.10.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.10.10.1, outside
C        10.10.10.0 255.255.255.0 is directly connected, outside
L        10.10.10.210 255.255.255.255 is directly connected, outside
B        10.255.254.255 255.255.255.255 [20/0] via 10.10.10.32, 00:01:31
B        10.255.255.255 255.255.255.255 [20/0] via 10.10.10.32, 00:01:31
C        192.168.45.0 255.255.255.0 is directly connected, inside
L        192.168.45.1 255.255.255.255 is directly connected, inside

> show bgp summary
BGP router identifier 192.168.45.1, local AS number 65001
BGP table version is 3, main routing table version 3
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 792 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.32     4        65536 49      40             3    0    0 00:40:38  2

>
```

Demo 7: Configuring OSPF on FDM

OSPF on FDM

For your reference

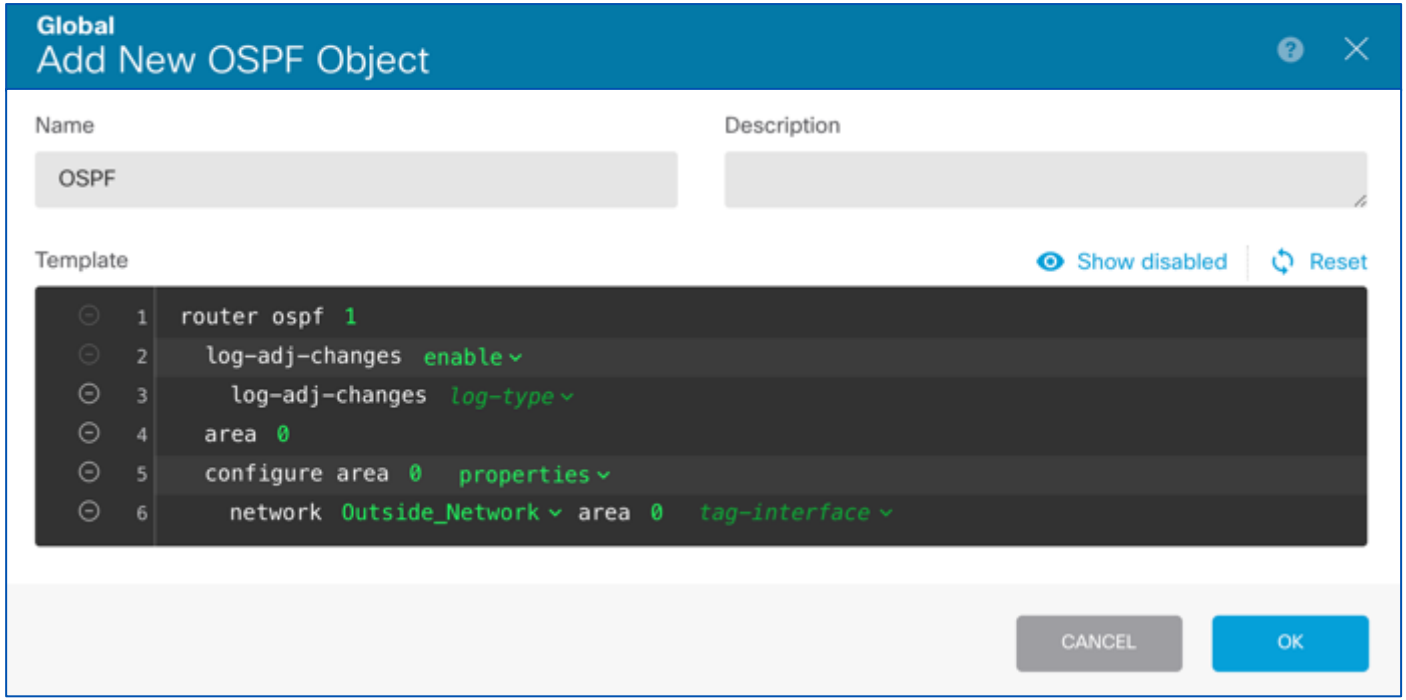
- Create OSPF Object



OSPF on FDM

For your reference

- Configure OSPF Object



OSPF on FDM

For your reference

- Verify routing table

```
CLI Console
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.10.10.1 to network 0.0.0.0

S*        0.0.0.0 0.0.0.0 [1/0] via 10.10.10.1, outside
C         10.10.10.0 255.255.255.0 is directly connected, outside
L         10.10.10.210 255.255.255.255 is directly connected, outside
B         10.255.254.255 255.255.255.255 [20/0] via 10.10.10.32, 01:03:08
B         10.255.255.255 255.255.255.255 [20/0] via 10.10.10.32, 01:03:08
O E2      192.168.30.0 255.255.255.0
            [110/20] via 10.10.10.30, 00:00:47, outside
C         192.168.45.0 255.255.255.0 is directly connected, inside
L         192.168.45.1 255.255.255.255 is directly connected, inside
```

Troubleshooting VRF

Troubleshooting - Commands

Configuration Verification

Global VRF	User- Defined VRF	All VRF
Show run route	Show run route vrf <name>	Show run route all
Show run router	Show run router vrf <name>	
Show run router bgp|ospf	Show run router bgp|ospf vrf <name>	Show run router bgp|ospf all

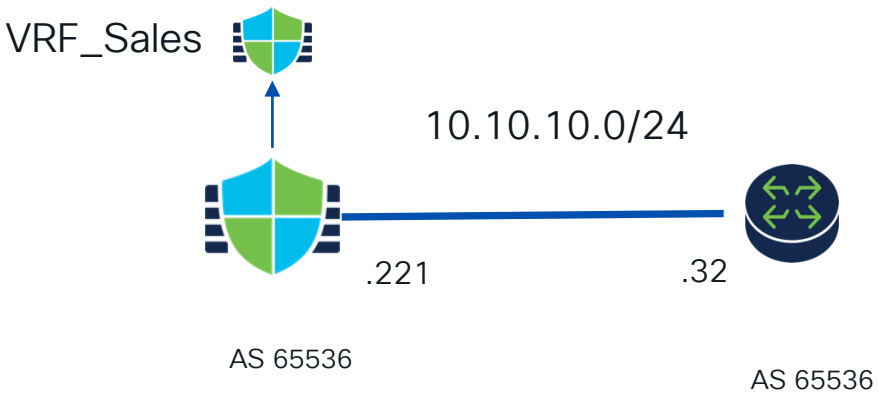
Troubleshooting - Commands

Troubleshooting Verification

Global VRF	User- Defined VRF	All VRF
Show route static|ospf|bgp	Show route static|ospf|bgp vrf <name>	Show route static|ospf|bgp all
Show bgp|ospf [sub-commands]	Show bgp|ospf vrf <name> [sub-commands]	

Troubleshooting Scenario #1 - BGP

- BGP won't come up



Demo 8: Troubleshooting Scenario #1 – BGP

Troubleshooting Scenario #1 - BGP

```
FTD67# sh run router
router bgp 65536
 bgp log-neighbor-changes
 bgp router-id vrf auto-assign
 address-family ipv4 unicast
  neighbor 10.10.10.23 remote-as 65526
  neighbor 10.10.10.23 transport path-mtu-discovery disable
  neighbor 10.10.10.23 activate
  no auto-summary
  no synchronization
 exit-address-family
```

```
FTD67# sh bgp summary
BGP router identifier 192.168.50.1, local AS number 65536
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.23     4        65526 0       0              1    0    0 never   Idle
```

Troubleshooting Scenario #1 – BGP

For your reference

```
FTD67# sh bgp neighbors

BGP neighbor is 10.10.10.23,  vrf single_vf,  remote AS 65526, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Neighbor sessions:
    0 active, is not multisession capable (disabled)
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 0
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:           0          0
    Prefixes Total:             0          0
    Implicit Withdraw:          0          0
    Explicit Withdraw:          0          0
    Used as bestpath:           n/a        0
    Used as multipath:          n/a        0
```

```
FTD67# ping 10.10.10.23
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.23, timeout is 2 seconds:
No route to host 10.10.10.23

Success rate is 0 percent (0/1)
FTD67# ping vrf vrf_sales 10.10.10.23
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.23, timeout is 2 seconds:
?????
```

Troubleshooting Scenario #1 – BGP

For your reference

```
FTD67# sh cap
capture capout type raw-data interface Outside [Capturing - 159 bytes]
  match tcp any any eq bgp
FTD67# sh cap capout

2 packets captured

   1: 16:56:06.942364       10.10.10.32.179 > 10.10.10.213.7130: P 2964002359:2964002378(19) ack 4068438279 win 16080
   2: 16:56:06.942440       10.10.10.213.7130 > 10.10.10.32.179: . ack 2964002378 win 32768
2 packets shown
```

```
FTD67# sh run router
router bgp 65536
 bgp log-neighbor-changes
 bgp router-id vrf auto-assign
 address-family ipv4 unicast
  neighbor 10.10.10.23 remote-as 65526
  neighbor 10.10.10.23 transport path-mtu-discovery disable
  neighbor 10.10.10.23 activate
  no auto-summary
  no synchronization
 exit-address-family
```

Troubleshooting Scenario #1 – BGP

For your reference

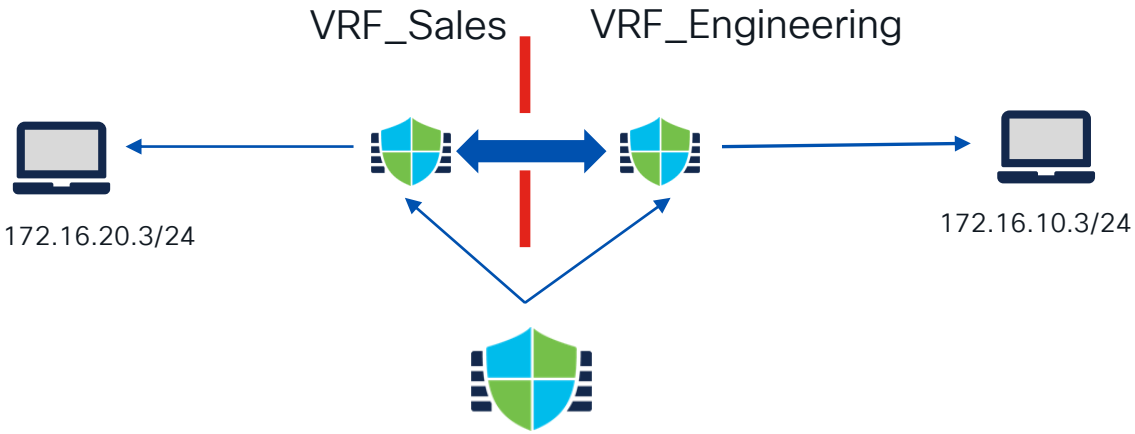
```
FTD67# sh route vrf vrf_sales


Routing Table: VRF_Sales
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.10.10.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.10.10.1, Outside
C        10.10.10.0 255.255.255.0 is directly connected, Outside
L        10.10.10.213 255.255.255.255 is directly connected, Outside
B        10.255.254.255 255.255.255.255 [200/0] via 10.10.10.32, 00:23:54
B        10.255.255.255 255.255.255.255 [200/0] via 10.10.10.32, 00:23:54
C        172.16.1.0 255.255.255.0 is directly connected, Sales
L        172.16.1.1 255.255.255.255 is directly connected, Sales
SI        172.16.2.0 255.255.255.0 [1/0] is directly connected, Engineering
O E2     192.168.30.0 255.255.255.0
           [110/20] via 10.10.10.30, 00:23:50, Outside
```

```
FTD67# show bgp vrf VRF_Sales summary
BGP router identifier 172.16.1.1, local AS number 65536
BGP table version is 3, main routing table version 3
2 network entries using 472 bytes of memory
2 path entries using 160 bytes of memory
1/1 BGP path/bestpath attribute entries using 224 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 856 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.32     4        65536 28      23             3    0    0 00:21:01  2
```

```
FTD67# ping vrf vrf_sales 10.255.254.255
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.254.255, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Troubleshooting Scenario #2

- Connectivity between VRFs (Route Leaking)



Demo 9: Troubleshooting Scenario #2

Troubleshooting Scenario #2 – Route Leak

For your reference

```
FTD67# sh run vrf

vrf VRF_Sales
vrf VRF_Engineering

FTD67# sh vrf

Name            VRF ID          Description             Interfaces
VRF_Sales               1                               Outside
                                                Sales
VRF_Engineering         2                               Engineering
FTD67# sh vrf ?

  WORD      Virtual Routing and Forwarding instance name
  counters  Show VRF counters
  lock      Show VRF lock information
  |         Output modifiers
  <cr>
FTD67# sh vrf cou
FTD67# sh vrf counters
Maximum number of VRFs supported: 29
Maximum number of IPv4 VRFs supported: 29
Maximum number of IPv6 VRFs supported: 29
Current number of VRFs: 2
Current number of VRFs in delete state: 0
```

```
FTD67# sh route vrf vrf_sales


Routing Table: VRF_Sales
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.10.10.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.10.10.1, Outside
C        10.10.10.0 255.255.255.0 is directly connected, Outside
L        10.10.10.213 255.255.255.255 is directly connected, Outside
B        10.255.254.255 255.255.255.255 [200/0] via 10.10.10.32, 04:07:38
B        10.255.255.255 255.255.255.255 [200/0] via 10.10.10.32, 04:07:38
C        172.16.1.0 255.255.255.0 is directly connected, Sales
L        172.16.1.1 255.255.255.255 is directly connected, Sales
SI        172.16.2.0 255.255.255.0 [1/0] is directly connected, Engineering
O E2     192.168.30.0 255.255.255.0
           [110/20] via 10.10.10.30, 04:07:34, Outside
```

Troubleshooting Scenario #2 – Route Leak

For your reference

```
FTD67# cap capin interface engineering match icmp any any
FTD67# cap capout interface sales  match icmp any any
```

```
FTD67# sh cap capin

4 packets captured

   1: 19:00:12.141456       172.16.2.3 > 172.16.1.3 icmp: echo request
   2: 19:00:16.802540       172.16.2.3 > 172.16.1.3 icmp: echo request
   3: 19:00:21.786351       172.16.2.3 > 172.16.1.3 icmp: echo request
   4: 19:00:26.777807       172.16.2.3 > 172.16.1.3 icmp: echo request
4 packets shown
FTD67# sh cap capout

0 packet captured

0 packet shown
```

Troubleshooting Scenario #2 – Route Leak

For your reference

```
FTD67# sh cap asp | in 172.16.1.3
  25: 18:53:14.100336       172.16.1.3.60926 > 8.8.8.8.53:  udp 34 Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x000055f275faf47d flow (NA)/NA
  26: 18:53:14.201954       172.16.1.3.60926 > 4.2.2.2.53:  udp 34 Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x000055f275faf47d flow (NA)/NA
  27: 18:53:15.204350       172.16.1.3.60926 > 8.8.8.8.53:  udp 34 Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x000055f275faf47d flow (NA)/NA
  29: 18:53:16.916136       172.16.2.3 > 172.16.1.3 icmp: echo request Drop-reason: (no-route) No route to host, Drop-location: frame 0x000055f275fb8149 flow (NA)/NA
  30: 18:53:17.206074       172.16.1.3.60926 > 8.8.8.8.53:  udp 34 Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x000055f275faf47d flow (NA)/NA
  31: 18:53:17.206105       172.16.1.3.60926 > 4.2.2.2.53:  udp 34 Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x000055f275faf47d flow (NA)/NA
  35: 18:53:21.226505       172.16.1.3.60926 > 8.8.8.8.53:  udp 34 Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x000055f275faf47d flow (NA)/NA
  36: 18:53:21.226550       172.16.1.3.60926 > 4.2.2.2.53:  udp 34 Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x000055f275faf47d flow (NA)/NA
  38: 18:53:21.800495       172.16.2.3 > 172.16.1.3 icmp: echo request Drop-reason: (no-route) No route to host, Drop-location: frame 0x000055f275fb8149 flow (NA)/NA
  43: 18:53:26.803959       172.16.2.3 > 172.16.1.3 icmp: echo request Drop-reason: (no-route) No route to host, Drop-location: frame 0x000055f275fb8149 flow (NA)/NA
  48: 18:53:31.793827       172.16.2.3 > 172.16.1.3 icmp: echo request Drop-reason: (no-route) No route to host, Drop-location: frame 0x000055f275fb8149 flow (NA)/NA
```

```
FTD67# sh run nat
nat (Sales,Engineering) source static Sales_Net Sales_Net destination static Eng_Network Eng_Network route-lookup
FTD67# sh run route vrf vrf_sales
route vrf VRF_Sales Outside 0.0.0.0 0.0.0.0 10.10.10.1 1
route vrf VRF_Sales Engineering 172.16.2.0 255.255.255.0 1
```

```
FTD67# packet-tracer input eng icmp 172.16.2.3 8 0  172.16.1.3

Result:
input-interface: Engineering(vrfid:2)
input-status: up
input-line-status: up
Action: drop
Drop-reason: (no-route) No route to host, Drop-location: frame 0x000055f275fb8149 flow (NA)/NA
```

Troubleshooting Scenario #2 – Route Leak

For your reference

packet-tracer input engineering icmp 172.16.2.3 8 0 172.16.1.3

Phase: 3
Type: INPUT-ROUTE-LOOKUP
 Subtype: Resolve Egress Interface
 Result: ALLOW
 Config:
 Additional Information:
 Found next-hop 0.0.0.0 using egress ifc Sales(vrfid:1)

Phase: 4
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Sales,Engineering) source static Sales_Net Sales_Net destination static Eng_Network Eng_Network route-lookup
Additional Information:
NAT divert to egress interface Sales(vrfid:1)
Untranslate 172.16.1.3/0 to 172.16.1.3/0

Troubleshooting Scenario #2 – Route Leak

For your reference

packet-tracer input engineering icmp 172.16.2.3 8 0 172.16.1.3

Phase: 18
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 172.16.1.3 using egress ifc Sales(vrfid:1)

Result:
input-interface: Engineering(vrfid:2)
input-status: up
input-line-status: up
output-interface: Sales(vrfid:1)
output-status: up
output-line-status: up
Action: allow

Troubleshooting Scenario #2 – Route Leak

For your reference

Connection Events (switch workflow)

2021-02-14 00:00:00 - 2021-02-16

Search Constraints (Edit Search)

Connections with Application Details | Table View of Connection Events

Jump to...

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2021-02-15 15:54:34	2021-02-15 15:54:34	Allow		172.16.2.3			172.16.1.3			Eng_zone	Sales_Zone	8 (Echo Request) / icmp	0 (No Code) / icmp

Access Control Policy	Access Control Rule	Network Analysis Policy	Prefilter Policy	Tunnel/Prefilter Rule	Source SGT	Destination SGT	Endpoint Profile	Endpoint Location	Device	Ingress Interface	Egress Interface	Ingress Virtual Router	Egress Virtual Router
ACP_CL	Eng_to_Sales	Balanced Security and Connectivity	Default Prefilter Policy						FTD 6.7	Engineering	Sales	VRF_Engineering	VRF_Sales

Conclusion

Conclusions

- Enhanced FTD's routing capabilities.
- Secure way of segmenting routing table and expands our FTD deployment options
- Take advantage of Meet the expert

- Let's deploy it!

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Thank you

cisco Live!

ALL IN

#CiscoLive