
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Firepower Threat Defense Virtual Routing and Forwarding (VRF)

Subtitle goes here

Luis Silva Benavides – Customer Success Specialist
@LuisSilva_1990

BRKSEC-2016

About your Speaker

Customer Success Specialist

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

Agenda

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

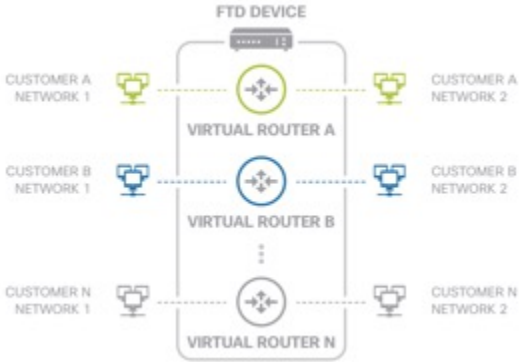
Introduction

Virtual Routing and Forwarding

cisco Live!

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 Not supported
Firepower 2100	10-40	
Firepower 4100	60-100	
Firepower 9300	60-100	
Virtual FTD	30	
ISA 3000	Not supported	

Configuration Guide

License required

No

Routing Policies

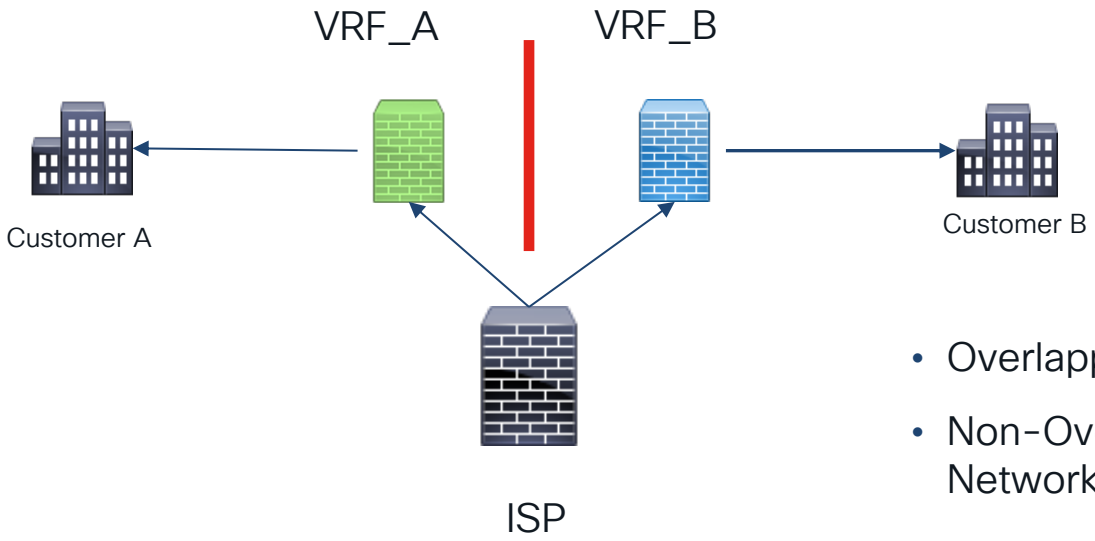
Policies	Global VRF	User VRF
Static Route	✓	✓
OSPFv2	✓	✓
OSPFv3	✓	✗
RIP	✓	✗
BGPv4	✓	✓
BGPv6	✓	✗
IRB (BVI)	✓	✓
EIGRP	✓	✗

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

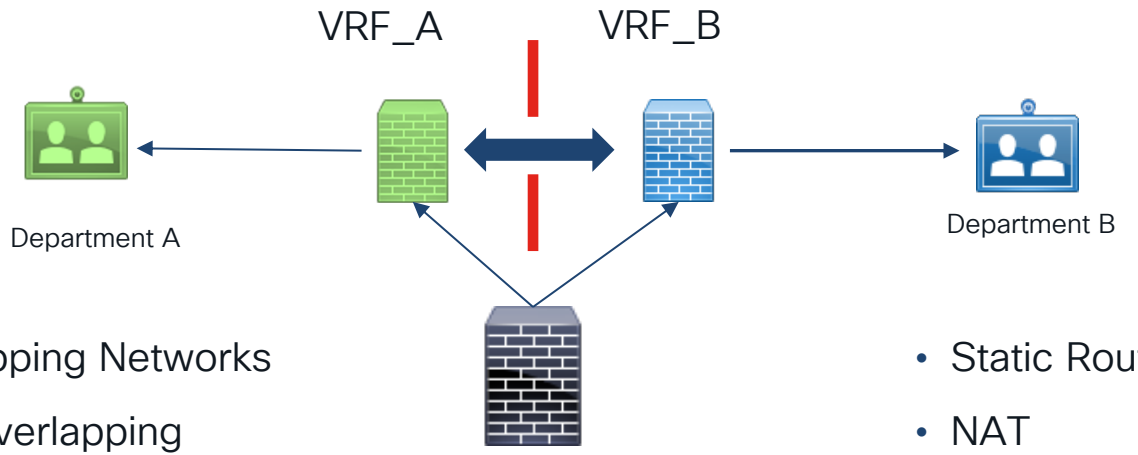
- Separate routing tables



- Overlapping Networks
- Non-Overlapping Networks

Use case #2 – Enterprise

- Connectivity between VRFs (Route Leaking)

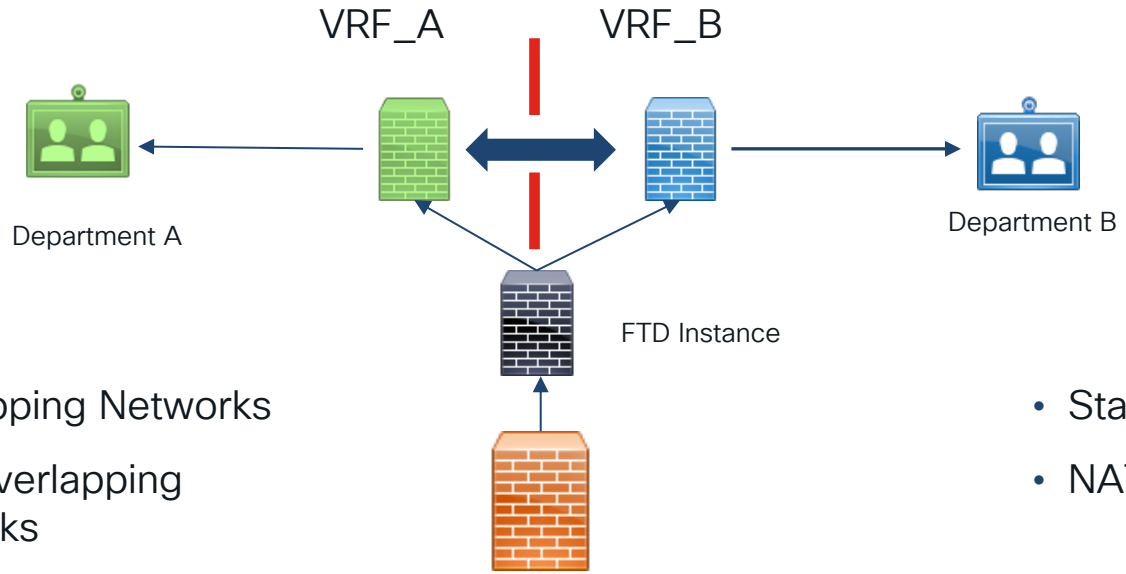


- Overlapping Networks
- Non-Overlapping Networks

- Static Routes
- NAT

Use case #3 – Multi-Instance and VRF

- Connectivity between VRFs in a Multi-Instance Environment



- Overlapping Networks
- Non-Overlapping Networks

- Static Routes
- NAT

Configuring VRF

Video 1: VRF configuration on FMC

Video 2: Configuring VRF on FDM

Configuring Routing Protocols

cisco Live!

Video 3: Configuring Static Routing on FMC

Video 4 : Configuring BGP on FMC

Video 5: Configuring OSPF on FMC

Video 6: Configuring BGP on FDM

Video 7: Configuring OSPF on FDM

Troubleshooting VRF

cisco Live!

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

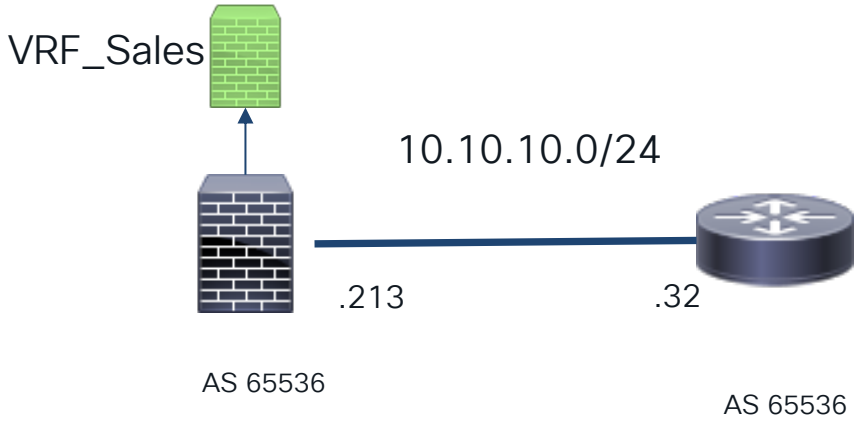
Troubleshooting - Commands

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

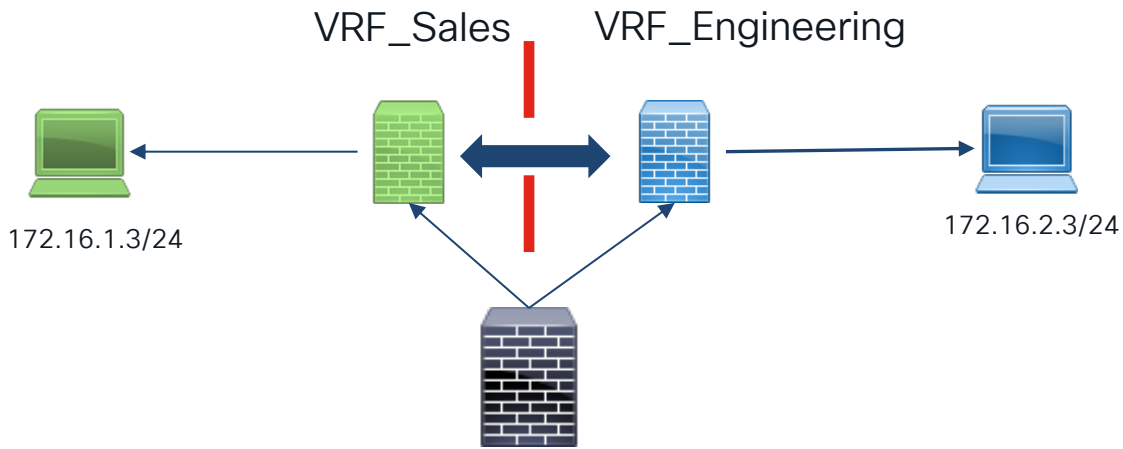
- BGP won't come up



Video 8: Troubleshooting Scenario #1 – BGP

Troubleshooting Scenario #2

- Connectivity between VRFs (Route Leaking)



Video 9: Troubleshooting Scenario #2

Conclusion

Conclusions

- Cisco DNA's embedded on FTD adding more routing capabilities.
- Expands our FTD deployment options
- Take advantage of Meet the expert

- Lets Test it and deploy it!

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive