Configure Dual ISP Failover for FTD Managed by FMC

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Static Route Tracking Feature Overview
Configure
Network Diagram
Configurations
<u>Verify</u>
Related Information

Introduction

This document describes how to configure DUAL ISP Failover with PBR and IP SLAs on an FTD that is managed by FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Policy Based Routing (PBR)
- Internet protocol service level agreement (IP SLA)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Components Used

The information in this document is based on these software and hardware versions:

- FMCv 7.3.0
- FTDv 7.3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Static Route Tracking Feature Overview

Static Route Tracking feature allows the FTD to use a connection to a secondary ISP in the event that the primary leased line becomes unavailable. In order to achieve this redundancy, the FTD associates a static route with a monitoring target that you define. The SSLA operation monitors the target with periodic ICMP echo requests.

If an echo reply is not received, then the object is considered down, and the associated route is removed from the routing table. A previously configured backup route is used in place of the route that is removed. While the backup route is in use, the SLA monitor operation continues its attempts to reach the monitoring target.

Once the target is available again, the first route is replaced in the routing table, and the backup route is removed.

You can now configure multiple next-hops and policy-based routing forwarding actions at the same time. When traffic matches the criteria for the route, the system attempts to forward traffic to the IP addresses in the order you specify, until it succeeds.

The feature is available on FTD devices running version 7.1 and later managed by an FMC version 7.3 and later.

Configure

Network Diagram

This image provides an example of a network diagram.



Image 1. Diagram example.

ISP1 = 10.115.117.1

ISP2 = 172.20.20.13

Configurations

Step 1. Configure the SLA Monitor objects.

On the FMC, navigate to Object > Object Management > SLA Monitor > Add SLA Monitor and add an SLA Monitor object for the ISP IP addresses.

SLA monitor for the primary default gateway (ISP1).

Name:		Description:	
SAL1			
Frequency (seconds):		SLA Monitor ID*:	
60		1	
(1-604800)			
Threshold (milliseconds):		Timeout (milliseconds):	
5000		5000	
(0-60000)		(0-604800000)	
Data Size (bytes):		ToS:	
28		0	
(0-16384)			
Number of Packets:		Monitor Address*:	
1		10.115.117.1	
Available Zones C			
Q Search		Selected Zones/Interfaces	
Backhone	Add	Outside	
Backup			
new			
Outside			
VI AN2816			
VEANZOID			
	,		

Image 2. SLA1 monitor configuration window.

SLA monitor for the secondary default gateway (ISP2).

Name:		Description:
SLA2		
Frequency (seconds):		SLA Monitor ID*:
60		2
(1-604800)		
Threshold (milliseconds):		Timeout (milliseconds):
5000		5000
(0-60000)		(0-604800000)
Data Size (bytes):		ToS:
28		0
(0-16384)		
Number of Packets:		Monitor Address*:
1		172.20.20.13
Available Zones a		
Q Search		Selected Zones/Interfaces
	- Add	
Backbone		Васкир
васкор		
new		
Outside		
VLAN2816		
·		

Image 3. SLA2 monitor configuration window.

Step 2. Configure the Static Routes with Route Track.

On the FMC, navigate to Device > Device Management > Edit the desired FTD > Routing > Static Routes, and add the statics routes with the correct SLA monitor.

The SLA monitor must be the one which monitors the default gateway.

Static route for the primary default gateway:

Type: IPv4 IPv6	
Interface* outside • (Interface starting with this icon is signifies it is available for route leak) Ausilable Network •	
Q Search Add anv-inv4	-
10.10.10.1 10.117.0.250 10.34.24.91 172.16.0.20 172.20.20.13 192.168.1.20	•
Ensure that egress virtualrouter has route to that destination	
Gateway	
10.115.117.1 • +	
Metric:	
1	
(1 - 254) Terrelate (, 4 - 4 - 4 - 4 - 4 - 4 - 4 - 4 - 4 - 4	
Route Tracking:	
SAL1 +	

Image 4. Static route configuration window for the Outside interface.

Static route for the secondary default gateway.

Edit Static Route Configuration	0
Type: IPv4 O IPv6 Interface* backup	
(Interface starting with this icon signifies it is available for route leak)	
Q Search Add any-ipv4	Ĩ
10.10.10.1 10.117.0.250 10.34.24.91 172.16.0.20 172.20.20.13 192.168.1.20	
Ensure that egress virtualrouter has route to that destination Gateway 172.20.20.13 + Metric: 254 (1 - 254) Tunneled: Used only for default Route) Route Tracking: SLA2 +	

Image 5. Static route configuration window for the Backup interface.

Step 3. Configure the Policy Base Routes.

 $Navigate \ to \ {\tt Device} > {\tt Device} \ {\tt Management} > {\tt Edit} \ {\tt the} \ {\tt desired} \ {\tt FTD} > {\tt Routing} > {\tt Policy} \ {\tt Based} \ {\tt Routing}, \ add \ the \ PBR, \ and \ choose$

the ingress interface.

Firewall Manageme Devices / Secure Firewall Re	nt Center Overview	Analysis Policies Devices Objects Integration	Deploy Q 💕 🌣 🕢 admin ~ 🕬 SECURE
FTDb-osmontoy Cisco Firepower Threat Defense for	or VMWare		You have unsaved changes Save Cancel
Device Routing Interfa	ces Inline Sets DHCP	лер	
Manage Virtual Routers	Policy Based Routing	Add Policy Based Route	ø
Global 👻	Specify ingress interfaces, match	A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces	Configure Interface Priority
Virtual Router Properties ECMP	Ingress Interfaces	Ingress Interface*	
BFD OSPF		Match Criteria and Egress Interface Seecify forward action for chosen match criteria. Add	
OSPFv3			
EIGRP			
Policy Based Routing			
∼ BGP			
IPv4			
IPv6		There are no forward-actions defined yet. Start by defining the first one.	
Static Route			
V Multicast Routing			
DIM			· ·
Multicast Routes		Cancel	
Multicast Boundary Filter			

Image 6. PBR configuration window.

Configure the forwarding actions.

- Choose or add a new access control list that you want to match.
- ChooseIP Address from the Send to option.
- In this example, 10.115.117.234 is the FTD outside IP address.

Edit Forwarding	Actions		0
Match ACL:*	all_ipv4_for_pbr ~ +		^
Send To:*	IP Address 🗸		
IPv4 Addresses:	10.115.117.234		
IPv6 Addresses:	For example, 2001:db8::, 2002:db8::1:		
Don't Fragment:	None		
Default Interface	e	I	
IPv4 settings	IPv6 settings		
Recursive:	For example, 192.168.0.1		- 1
Default:	For example, 192.168.0.1, 10.10.10.1		
Peer Address			
Verify Availability		+	-
		Cancel	Save

Image 7. Forwarding Actions configuration window.

Scroll down and add the Verify Availability values for ISP1.

Edit Forwardin	g Actions		0
 Default Interfa 	ce		*
IPv4 settings	IPv6 settings		
Recursive:	For example, 192.168.0.1		
Default:	For example, 192.168.0.1, 10.10.10.1		
Peer Address			
Verify Availability	,		+
IP Address:	Sequence:	Track:	
10.115.117.1	1	1	/1
			Cancel Save

Image 8. Forwarding Actions configuration window.

Repeat the same process for the backup interface. However, ensure to use a different access control list object.

Edit Forwarding	Actions		0
Match ACL:* Send To:* IPv4 Addresses: IPv6 Addresses: Don't Fragment:	internal_networks ✓ IP Address ✓ 172.20.20.77 ✓ For example, 2001:db8::, 2002:db8::1; ✓ None ✓		A
Default Interfact IPv4 settings	e IPv6 settings		
Recursive: Default:	For example, 192.168.0.1 For example, 192.168.0.1, 10.10.10.1		
Verify Availability		+	Ŧ
		Cancel	Save

Repeat the same process for the Verify Availability configuration but now for ISP2.

Edit Forwardin	g Actions		0
Default Interfa	ce		•
IPv4 settings	IPv6 settings		
Recursive:	For example, 192.168.0.1		
Default:	For example, 192.168.0.1, 10.10.10.1		
Peer Address			
Verify Availability			+
IP Address:	Sequence:	Track:	
172.20.20.13	2	2	/1
L			
			•
			Cancel Save

Image 10. Verify Availability configuration.

Validate your configuration.

Firewall Manageme Devices / Secure Firewall Ro	nt Center couting	Overview	Analysis	Policies	Devices	Objects	Integration				Deploy	۹ (¢ 💡	@ adm	nin v 🔤	tisce SECURE
FTDb-osmontoy Cisco Firepower Threat Defense fo	r VMWare	DUCD	VITED													Cancel
Manage Virtual Routers	Policy Based F Specify ingress inter	Routing rfaces, match	h criteria and	egress interfa	ces to route tr	affic accordir	ngly. Traffic can be ro	uted across Egre:	ss interfaces accordin	gly			Configura	Interface P	Prioritu	Add
Virtual Router Properties	Ingress Interfaces				Mat	tch criteria and	forward action						Joundana	INGING P	nonty	Pad
BFD	vlan2816				If to all_	affic matches the ipv4_for_pbr	he Access List		Send ti 10.115	rough 117.234						/1
OSPFv3					If to Inte	affic matches the	he Access List s		Send ti 172.20	rough 20.77						
RIP																

Image 11. PBR configuration.

Verify

Access the FTD through Secure Shell (SSH) and use the command system support disagnotsic-cli and run these commands:

• show route-map: This command displays the route-map configuration.

firepower#

show route-map

```
route-map FMC_GENERATED_PBR_1679065711925
```

```
, permit, sequence 5
Match clauses:
ip address (access-lists): internal_networks
```

```
Set clauses:
ip next-hop verify-availability 10.115.117.1 1
```

track 1 [up]

```
ip next-hop 10.115.117.234
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr
```

```
Set clauses:
ip next-hop verify-availability 172.20.20.13 2
```

track 2 [up]

```
ip next-hop 172.20.20.77
firepower#
```

• show running-config sla monitor: This command displays the SLA configuration.

<#root>

```
firepower#
```

show running-config sla monitor

sla monitor 1

type echo protocol ipIcmpEcho 10.115.117.1 interface outside sla monitor schedule 1 life forever start-time now

sla monitor 2

```
type echo protocol ipIcmpEcho 172.20.20.13 interface backup
sla monitor schedule 2 life forever start-time now
firepower#
```

• show sla monitor configuration: This command displays the SLA configuration values.

```
firepower#
```

show sla monitor configuration

SA Agent, Infrastructure Engine-II Entry number:

1

Owner: Tag: Type of operation to perform: echo

Target address: 10.115.117.1

```
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

Entry number:

2

Owner: Tag: Type of operation to perform: echo

Target address: 172.20.20.13

```
Interface: backup
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

• show sla monitor operational-state: This command displays the operational state of the SLA operation.

firepower# show sla monitor operational-state Entry number: 1 Modification time: 15:48:04.332 UTC Fri Mar 17 2023 Number of Octets Used by this Entry: 2056 Number of operations attempted: 74 Number of operations skipped: 0 Current seconds left in Life: Forever Operational state of entry: Active Last time this entry was reset: Never Connection loss occurred: FALSE Timeout occurred: FALSE Over thresholds occurred: FALSE Latest RTT (milliseconds): 1 Latest operation start time: 17:01:04.334 UTC Fri Mar 17 2023 Latest operation return code: OK RTT Values: RTTAvg: 1 RTTMin: 1 RTTMax: 1 NumOfRTT: 1 RTTSum: 1 RTTSum2: 1 Entry number: 2 Modification time: 15:48:04.335 UTC Fri Mar 17 2023 Number of Octets Used by this Entry: 2056 Number of operations attempted: 74 Number of operations skipped: 0 Current seconds left in Life: Forever Operational state of entry: Active Last time this entry was reset: Never Connection loss occurred: FALSE Timeout occurred: FALSE Over thresholds occurred: FALSE Latest RTT (milliseconds): 1 Latest operation start time: 17:01:04.337 UTC Fri Mar 17 2023 Latest operation return code: OK RTT Values: RTTAvg: 1 RTTMin: 1 RTTMax: 1 NumOfRTT: 1 RTTSum: 1 RTTSum2: 1 • show track: This command displays the information about objects tracked by the SLA Track process.

<#root>

<#root>

firepower#

show track

Track 1 Response Time Reporter 1 reachability Reachability is Up 4 changes, last change 00:53:42 Latest operation return code: OK Latest RTT (millisecs) 1 Tracked by: ROUTE-MAP 0 STATIC-IP-ROUTING 0 Track 2 Response Time Reporter 2 reachability Reachability is Up 2 changes, last change 01:13:41 Latest operation return code: OK Latest RTT (millisecs) 1 Tracked by: ROUTE-MAP 0 STATIC-IP-ROUTING 0

• show running-config route: This command displays the current route configuration.

<#root>

firepower#

show running-config route

route

outside

0.0.0.0 0.0.0.0 10.115.117.1 1

track 1

route

backup

0.0.0.0 0.0.0.0 172.20.20.13 254

track 2

route vlan2816 10.42.0.37 255.255.255.255 10.43.0.1 254 firepower#

• show route: This command displays the routing table for the data interfaces.

<#root>

firepower#

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, BI - BGP InterVRF
Gateway of last resort is 10.115.117.1 to network 0.0.00
```

s* 0.0.0.0 0.0.0.0 [1/0] via 10.115.117.1, outside

```
S 10.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone
C 10.88.243.0 255.255.255.0 is directly connected, backbone
L 10.88.243.67 255.255.255.255 is directly connected, backbone
C 10.115.117.0 255.255.255.0 is directly connected, outside
L 10.115.117.234 255.255.255.255 is directly connected, outside
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816
C 172.20.20.0 255.255.255.0 is directly connected, backup
L 172.20.20.77 255.255.255 is directly connected, backup
```

When the primary link fails:

• show route-map: This command displays the route-map configuration when a link fails.

<#root>

firepower#

show route-map FMC_GENERATED_PBR_1679065711925

route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 5
Match clauses:
ip address (access-lists): internal_networks

Set clauses: ip next-hop verify-availability 10.115.117.1 1

track 1 [down]

ip next-hop 10.115.117.234
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr
Set clauses:
ip next-hop verify-availability 172.20.20.13 2
track 2 [up]

ip next-hop 172.20.20.77
firepower#

• show route: This command displays the new routing table per interface.

<#root>

firepower#

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, BI - BGP InterVRF
Gateway of last resort is 10.115.117.1 to network 0.0.00
```

S* 0.0.0.0 0.0.0.0 [1/0] via 172.20.20.13, backup

S 10.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone C 10.88.243.0 255.255.255.0 is directly connected, backbone L 10.88.243.67 255.255.255.0 is directly connected, backbone C 10.115.117.0 255.255.255.0 is directly connected, outside L 10.115.117.234 255.255.255.255 is directly connected, outside C 10.42.0.0 255.255.255.0 is directly connected, vlan2816 L 10.42.0.1 255.255.255.255 is directly connected, vlan2816 S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816 C 172.20.20.0 255.255.255.0 is directly connected, backup L 172.20.20.77 255.255.255 is directly connected, backup

Related Information

- <u>Cisco Secure Firewall Management Center Administration Guide, 7.3</u>
- <u>Technical Support & Documentation Cisco Systems</u>