為FMC管理的FTD配置雙ISP故障切換

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>靜態路由跟蹤功能概述</u> <u>設定</u> <u>網路圖表</u> <u>組態</u> <u>驗證</u> <u>相關資訊</u>

簡介

本檔案介紹如何在FMC管理的FTD上使用PBR和IP SLA設定雙ISP容錯移轉。

必要條件

需求

思科建議您瞭解以下主題:

- 原則型路由(PBR)
- 網際網路通訊協定服務等級協定(IP SLA)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- FMCv 7.3.0
- FTDv 7.3.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

靜態路由跟蹤功能概述

靜態路由跟蹤功能允許FTD在主租用線路不可用時使用與輔助ISP的連線。為了達到此備援,FTD將 靜態路由與您定義的監控目標相關聯。SSLA操作使用定期的ICMP回應請求監控目標。

如果沒有收到回應應答,則會將該對象視為關閉,並從路由表中刪除關聯的路由。使用先前配置的 備份路由來代替已移除的路由。使用備份路由時,SLA監控操作將繼續嘗試訪問監控目標。

目標再次可用後,第一個路由將替換在路由表中,備份路由將被刪除。

現在,您可以同時配置多個下一跳和基於策略的路由轉發操作。當流量與路由的條件匹配時,系統 將嘗試按照您指定的順序將流量轉發到IP地址,直到成功。

此功能在運行7.1版及更高版本、由FMC 7.3版及更高版本管理的FTD裝置上可用。

設定

網路圖表

此圖提供網路圖示範例。



圖1.圖示示例。

ISP1 = 10.115.117.1

ISP2 = 172.20.20.13

組態

步驟 1.配置SLA監控器對象。

在FMC上,導航至 Object > Object Management > SLA Monitor > Add SLA Monitor 並為ISP IP地址新增SLA

Monitor對象。

主預設網關(ISP1)的SLA監控。

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
Backbone	Add	Outside
Backup		
new		
Outside		
VLAN2816		

圖2.SLA1監控器配置視窗。

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

步驟 2.使用路由跟蹤配置靜態路由。

在FMC上, 導航至 Device > Device Management > Edit the desired FTD > Routing > Static Routes 並使用正確的SLA監控器 新增靜態路由。

SLA監控器必須是監控預設網關的監控器。

主預設網關的靜態路由:

Edit Static Route Configuration	0
Type: IPv4 IPv6	
outside	
(Interface starting with this icon signifies it is available for route leak)	
Available Network C + Selected Network	
Q Search Add any-ipv4	Ì
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)	
Tunneled: Used only for default Route)	
SAL1 +	

圖4.外部介面的靜態路由配置視窗。

輔助預設網關的靜態路由。

Edit Static Route Configuration	0
Type: IPv4 O IPv6	
Interrace"	
backup	
(Interface starting with this icon Signifies it is available for route leak)	
Available Network C + Selected Network	
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 • +	

圖5.備用介面的靜態路由配置視窗。

步驟 3.配置策略基本路由。

導航至 Device > Device Management > Edit the desired FTD > Routing > Policy Based Routing,新增PBR,並選擇輸入介面

Devices / Secure Firewall Ro	nt Center Overview	Analysis Policies Devices Objects Integration	Deploy Q 🗳 🌣 🕢 admin 🗸 🕬 SECURE
FTDb-osmontoy Cisco Firepower Threat Defense for	r VMWare	759	You have unsaved changes Save Cancel
Device Rodding Internal	Ces mane Sets Drice		•
Manage Virtual Routers	Policy Based Routing	Add Policy Based Route	
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 Add
Virtual Router Properties		Ingress Interface*	
ECMP	ingress interfaces	Select V	
BFD			
OSPE		Match Criteria and Egress Interface	
OSPEv3		Specify forward action for chosen match criteria.	
FIGRP			
RIP			
Policy Based Routing			
∼ BGP			
IPv4			
IPv6		There are no forward-actions defined yet. Start by defining the first one.	
Static Route			1
Multicast Routing			
IGMP			
PIM			
Multicast Routes		Cancel Save	
Multicast Boundary Filter			

圖6.PBR配置視窗。

配置轉發操作。

- 選擇或新增要匹配的新訪問控制清單。
- 選擇IP Address 從 Send to 選項。
- 在本範例中,10.115.117.234是FTD內部IP位址。

Edit Forwarding	Actions		0
Match ACL:*	all_ipv4_for_pbr v +		^
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)		
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		+	-
		Cancel	•

圖7.Forwarding Actions配置視窗。

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

圖8.Forwarding Actions配置視窗。

對備份介面重複相同的過程。但是,請確保使用不同的訪問控制清單對象。

Edit Forwarding	Actions		0
Match ACL:*	internal_networks v +		A
Send To:*	IP Address		
IPv4 Addresses:	172.20.20.77		
IPv6 Addresses:	For example, 2001:db8::, 2002:db8::1:		
Don't Fragment:	None		
Default Interface)		
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		+	Ŧ
		Cancel	

對重複相同的過程Verify Availability配置,但現在用於ISP2。

Edit Forwardin	g Actions		0
Default Interfa	ce		A
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

映像10.驗證可用性配置。

驗證您的配置。

Firewall Management Devices / Secure Firewall Roo	nt Center	Overview	Analysis	Policies	Devices	Objects	Integration			Deploy	۹ (¢ 💡	0	admin \sim	-dr.dr. Cisco	SECURE
FTDb-osmontoy Cisco Firepower Threat Defense for Device Routing Interface	VMWare es Inline Sets	DHCP	VTEP												are	Cancel
Manage Virtual Routers	Policy Based Specify ingress inte	Routing erfaces, matc	h criteria and	egress interfac	ces to route tr	affic accordin	gly. Traffic can be routed a	across Egress interfaces a	cordingly			Configur	e Interfa	ce Priority		Add
Virtual Router Properties	Ingress Interfaces				Ma	tch criteria and	forward action									
ecmp BFD OSPF	vlan2816				if tr all_	affic matches th ipv4_for_pbr	e Access List		Send through 10.115.117.234						1	Ŷ
OSPFv3					lif tr	affic matches th	e Access List		Send through							
EIGRP					inte	rnai_networks			172.20.20.77							
KOP	·															

圖11.PBR配置。

驗證

透過安全殼層(SSH)存取FTD,並使用命令 system support disagnotsic-cli 並運行以下命令:

• show route-map:此命令顯示路由對映配置。

<#root>

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:此命令顯示SLA配置。

<#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:此命令顯示SLA配置值。

<#root>

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:此命令顯示SLA操作的運行狀態。

<#root>

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:此命令顯示有關SLA跟蹤進程跟蹤的對象的資訊。

<#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:此命令顯示當前路由配置。

<#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:此命令顯示資料介面的路由表。

<#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 10.0.0.0 255.0.0.0 [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

當主鏈路發生故障時:

• show route-map:此命令在鏈路發生故障時顯示路由對映配置。

<#root>

firepower#

show route-map FMC_GENERATED_PBR_1679065711925

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

ip next-hop 1/2.20.20.// firepower#

• show route:此命令顯示每個介面的新路由表。

<#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 10.0.0.0 255.0.0.0 [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

相關資訊

- 思科安全防火牆管理中心管理指南7.3
- <u>技術支援與文件 Cisco Systems</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。