# 在Azure FTD中部署冗餘資料介面,由CD-FMC管 理

# 目錄

# 簡介

本檔案介紹設定cdFMC管理的虛擬FTD以使用備援管理員存取資料介面功能的步驟。

# 必要條件

需求

思科建議您瞭解以下主題:

- Cisco安全防火牆管理中心
- Cisco Defense Orchestrator

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 雲端提供的防火牆管理中心
- 託管在Azure雲中的虛擬安全防火牆威脅防禦7.3.1版。

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。

# 相關產品

本文件也適用於以下硬體和軟體版本:

• 任何能夠運行Firepower威脅防禦7.3.0版或更高版本的物理裝置。

# 背景資訊

本文檔顯示配置和驗證cdFMC管理的vFTD的步驟,以便使用兩個資料介面進行管理。當客戶需要 使用第二個ISP透過網際網路來管理其FTD時,此功能通常非常有用。預設情況下,FTD會對兩個介 面之間的管理流量執行輪詢負載平衡;這可修改為作用中/備份部署,如本檔案所述。

安全防火牆威脅防禦7.3.0版中引入了用於管理的冗餘資料介面功能。假設vFTD可以連線到可以解

# 析CDO存取URL的名稱伺服器。

# 組態

# 網路圖表



網路圖表

# 配置用於管理訪問的資料介面

透過控制檯登入裝置,然後使用configure network management-data-interface命令為管理訪問配置 一個資料介面:

#### <#root>

#### >

#### configure network management-data-interface

Note: The Management default route will be changed to route through the data interfaces. If you are consistent interface with SSH, your connection may drop. You must reconnect using the console port.

Data interface to use for management:

#### GigabitEthernet0/0

Specify a name for the interface [outside]:

outside-1

IP address (manual / dhcp) [dhcp]:

manual

IPv4/IPv6 address:

10.6.2.4

Netmask/IPv6 Prefix:

255.255.255.0

Default Gateway:

10.6.2.1

請記住,原始管理介面不能配置為使用DHCP。可以使用命令show network 對此進行驗證。

# 使用CDO載入FTD

此過程在帶有CDO的Azure FTD中內建,以便可由雲交付的FMC管理。此過程使用CLI註冊金鑰 ,如果您的裝置透過DHCP分配了IP地址,則此金鑰將非常有用。只有Firepower 1000、Firepower 2100或Secure Firewall 3100平台支援其他自註冊方法,如日誌觸控調配和序列號。

步驟 1.在CDO門戶中,導航到資產,然後點選板載選項:

÷	$\rightarrow$ C		08-	≏ https://www. <b>d</b>	efenseorch	nestrator.co	om/devices						☆		◙	$\mathbf{F}$	»	്	=
-ili-ili- cisco	Defense Orchestra	itor	Invento	ory			Q Searc	ch		<b>⊳</b> ,	۵.	4	? -						
≡	Hide Menu		T Dev	vices Templates	s Q	Search by	Device Nam	ie, IP Address,	or Serial Nun	nber			Disp	playing 0 of 0	) results			9	+
	Dashboard		All																2
$\bigcirc$	Multicloud Ner Defense	w		Name 🗘						Configuratio	n Status 🗘			Connectivity	, •				
	Inventory		1																-
Con	figuration																		
۲	Policies	>																	
$\diamond$	Objects	>																	
°Ç0	VPN	>																	
Ever	nts & Monitoring																		
	Analytics	>				No devi	ces or servic	ces found. You	must onboar	d a device o	or service t	o get sta	irted.						
٢	Change Log																		
( <u>+</u> )	Jobs																		
X	Tools & Services	>																	
{\$}	Settings	>																	

資產頁面

步驟2.按一下FTD方塊中的:





# 第3步:選擇使用CLI註冊金鑰選項:

A Important: After onboarding your FTD, it will be managed by Firewall Management Center in CDO. Note that use of the firewall device FTD 0000 manager will not be available after onboarding, and all existing policy configurations will be reset. You will need to reconfigure polices from CDO after onboarding. Learn more 🗹 **Firewall Threat Defense** <del>...</del> Deploy an FTD to a cloud Use CLI Registration Key Use Serial Number Use this method for low-touch Onboard a device using a registration environment key generated from CDO and applied on the device using the Command provisioning or for onboarding configured devices using their serial Deploy an FTD to a supported cloud onment; AWS, GCP and Azure Line Interfac (FTD 7.2+) (FTD 7.0.3+ & 7.2+)

使用CLI註冊金鑰

步驟 4.從configure manager命令開始複製CLI金鑰:

1	Device Name	FTDv-Azure
2	Policy Assignment	Access Control Policy: Default Access Control Policy
3	Subscription License	Performance Tier: FTDv, License: Threat, Malware, URL License
4	CLI Registration Key	<ul> <li>Ensure the device's initial configuration is complete before trying to apply the registration key. Learn more C</li> <li>Copy the CLI Key below and paste it into the CLI of the FTD</li> <li>configure manager add cisco-cisco-systemss1kaau.app.us.cdo.cisco.com t67mPqC8cAW6GH2NhhhTUD4poWARdRr7 YJqFWzmpnfbJ6WANBeHTAhXnod9E7cle cisco-cisco-systemss1kaau.app.us.cdo.cisco.com</li> </ul>
		Next

Copy Configure Manager命令



註:CLI金鑰與使用內部FMC註冊FTD時使用的格式相匹配,在註冊過程中,您可以配置

NAT-ID,以便在受管裝置位於NAT裝置之後時允許註冊:configure manager add <fmchostname-or-ipv4> <registration-key> <nat-id> <display-name>

步驟 5.將命令貼入FTD CLI。如果通訊成功,您必須接收此消息:

Manager cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com successfully configured. Please make note of reg\_key as this will be required while adding Device in FMC.

# 步驟 6.返回CDO,然後按一下下一步:

3	Subscription License	Performance Tier: FTDv, Licen
4	CLI Registration Key	1 Ensure the device's initial 2 Copy the CLI Key below an configure manager add t67mPqC8cAW6GH2NhhhTL systemss1kaau.app.t
		Next

按一下「下一步」

CDO會繼續執行註冊程式,並顯示一則訊息,指出需要很長時間才能完成。您可以點選服務頁面中 的裝置連結來檢查註冊過程的狀態。

步驟 7.透過工具和服務頁面訪問FMC。



存取cdFMC

# 按一下Devices連結。

Management							
	Devices Policies Objects						
÷.	NAT Site to Site VPN						
ф Э	Remote Access VPN Platform Settings						

按一下「裝置」

您的FTD現在已登入CDO,可由雲端提供的FMC管理。請注意下一個影像中的裝置名稱下列出NO-IP。在使用CLI註冊金鑰的自行啟用過程中,這是預期結果。

Control Part Price Analysian Control Price Analysian Analysian Analysian Control Price Analysian	s Policies Device	es Objects Integrat	ion *> Return Home Deploy Q	o 🔅 🛛	cisco SECURE
View By: Group  All (1)  Error (0)  Warning (0)  Offline (0)	Normal (1)	Deployment Pending (0)	Upgrade (0)     Snort 3 (1)	(	Deployment History
Collarse All					
Name	Model	Version Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)					
FTDv-Azure Snort 3     NO-IP - Routed	FTDv for Azure	7.3.1 N/A	Essentials, IPS (2 more)	Default Access Control Policy	∅ 1:

# 為Manager訪問配置冗餘資料介面

# 此過程為管理訪問分配第二個資料介面。

步驟 1.在Devices索引標籤中,按一下鉛筆圖示以存取FTD編輯模式:

Defense Orchestrator Analysis FMC / Devices / Device Management Analysis	Policies Devices	Objects Integration +> Ret	um Home Deploy Q	o 🌣 🛛	cisco SEC	URE
View By: Group •					Deployment Histo	yry
All (1) • Error (0) • Warning (0) • Offline (0)	Normal (1)	eployment Pending (0) • Upgrade (0	) • Snort 3 (1)	a	Search Device Ad	d 💌
Collapse All						
Name	Model	Version Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)						
FTDv-Azure Snort 3     NO-IP - Routed	FTDv for Azure 7	7.3.1 N/A	Essentials, IPS (2 more)	Default Access Control Policy	«9	11

編輯FTD

步驟 2.在Interface頁籤中,編輯將分配為冗餘管理介面的介面。如果之前沒有這樣做,請配置介面 名稱和IP地址。

步驟 3.在Manager Access 頁籤中,啟用Enable management on this interface for the manager 覈 取方塊:

Edit Physic	cal Interf	ace						0
General	IPv4	IPv6	Path Monitor	ing Hardwa	are Configuration	Manager Access	Advanced	
Inable m	anagemer	nt on this i	nterface for the	e Manager				
Available Net	works C		+		Allo	wed Management Netv	vorks	
Q Search					ar	ny		
any-ipv4								
any-ipv6				Add	d			
IPv4-Bench	mark-Test	s						
IPv4-Link-L	.ocal							
IPv4-Multic	ast							
IPv4-Privat	e-10.0.0.0	-8						
							[	Cancel

啟用管理員存取

步驟 4.在常規頁籤中,確保將介面分配給安全區域,然後按一下確定:

#### Edit Physical Interface

General	IPv4	IPv6	Path Monitoring	Hardware Configuration	Manager Access	Advanced
Name:						
outside-2						
Enabled						
Managem	nent Only					
Description:						
Mode:						
None			•			
Security Zone	):		_			
outside2-sz	z		*			

冗餘資料介面的安全區域

步驟 5.請注意,現在兩個介面都有Manager Access標籤。此外,請確定已將主要資料介面指派給不同的安全區域:

F7 Cis	<b>FDv-A</b> co Firepo	ZUIE wer Threat D	efense for Azur	e								Save	Cancel
1	Device	Routing	Interfaces	Inline Sets	DHC	P VTEP							
								Q Se	arch by name	Sync	Device	Add Inter	rfaces 🔻
	Interface	9		Logical N	Тур	Security Z	MAC Address (Active/Standby)		IP Address		Path	Virtual Ro	
	<ul> <li>Diagn</li> </ul>	ostic0/0		diagnostic	Phy						Disa	Global	/
	🔵 Gigab	itEthernet0/0	(Manager Access)	outside-1	Phy	outside1-sz			10.6.2.4/255.255.255.0(Static)		Disa	Global	/
	🔵 Gigat	itEthernet0/1	(Manager Access)	outside-2	Phy	outside2-sz			10.6.3.4/255.255.255.0(Static)		Disa	Global	/

介面配置檢查

在下一節中,步驟6到步驟10用於配置兩個等價預設路由以到達CDO,每個路由都由獨立的SLA跟 蹤進程監控。SLA跟蹤確儲存在使用受監控介面與cdFMC通訊的功能路徑。

步驟 6.導航到路由頁籤,然後在ECMP選單下建立包含兩個介面的新ECMP區域:



配置ECMP區域

按一下OK 和Save。

步驟 7.在Routing 頁籤中,導航到Static Routes。

點選鉛筆圖示可編輯您的主要路由。然後按一下加號以增加新的SLA跟蹤對象:

FTDv-Azure	Ym	have unsaved changes Save Cancel
Cisco Firepower Threat Defense for Azure	Edit Static Route Configuration	
Device Routing Interfaces Inlin	Type:      IPv4      IPv6  Interface*	
Manage Virtual Routers	outside-1	+ Add Route
Global • Networ	(Interface starting with this icon 👩 signifies it is available for route leak)	fetric Tracked
Virtual Router Properties	Available Network C + Selected Network	
ECMP BFD	Q Search Add any-ipv4	2 🗾
OSPF VIPve	IPv4-Benchmark-Tests IPv4-Link-Local	
EIGRP	IPv4-Multicast IPv4-Private-10.0.0-8	
Policy Based Routing V BGP	IPv4-Private-172.16.0.0-12	
IPv4 IPv6 Static Route	Ensure that egress virtualrouter has route to that destination Gateway	
<ul> <li>Multicast Routing</li> <li>IGMP</li> <li>PIM</li> </ul>	Metric:	
Multicast Routes Multicast Boundary Filter	Tunneled: Ulsed only for default Route) Route Tracking:	
General Settings BGP	Cancel OK	of 1 > >  C

編輯主要路由以增加SLA跟蹤

步驟 8.功能性SLA跟蹤所需的引數在下一幅圖中突出顯示。或者,您可以調整其他設定,如資料包 數、超時和頻率。

Name: outside1-sla		Description:
Frequency (seconds): 60 (1-604800)		SLA Monitor ID*:
Threshold (milliseconds): 5000		Timeout (milliseconds): 5000 (0-604800000)
Data Size (bytes): 28		ToS: 0
Number of Packets:		Monitor Address*:
Available Zones C Q Search	Add	Selected Zones/Interfaces
outside1-sz outside2-sz		outside1-sz
		Cancel Save

0

在本例中,Google DNS IP用於監控透過outside1介面訪問Internet(和CDO)的FTD功能。準備就 緒時,按一下ok。



附註:確認您正在追蹤已從FTD外部介面驗證為可連線的IP。使用無法連線的IP設定追蹤可 能會使此FTD中的預設路由停用,然後妨礙其與CDO通訊的能力。

步驟 9.按一下Save, 並確保新的SLA跟蹤已分配給指向主介面的路由:

# Route Tracking:

outside1-sla

按一下OK後,將顯示一個彈出窗口,其中包含下一條警告消息:

# Warning about Static Route

This Static route is defined on the Defense Orchestrator Access Interface. Ensure the change is not affecting connectivity to the device



配置警告

步驟 10.按一下Add Route選項為冗餘資料介面增加新路由。注意,從下一個映象中,路由的 Metric值相同;此外,SLA跟蹤具有不同的ID:

Type:      IPv4      IPv6	
Interface*	
outside-2	
(Interface starting with this icon signifies it is ava	ilable for route leak)
Available Network C +	Selected Network
Q Search Add	any-ipv4
any-ipv4	
IPv4-Benchmark-Tests	
IPv4-Link-Local	
IPv4-Multicast	
IPv4-Private-10.0.0.0-8	
IPv4-Private-172.16.0.0-12	
Gateway*	
10.6.3.1 ▼ +	
Metric:	
1	
(1 - 254)	
Tunneled: (Used only for default Route)	
Route Tracking:	
outside2-sla 🔹 +	
	Canad

配置冗餘靜態路由

Name:	-	Description:
outside2-sla	J	
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		
Available Zones C		
Q Search		Selected Zones/Interfaces
outside1-sz	Add	outside2-sz
outside2-sz		
1		
		Cancel Save

0

### 按一下Save。

步驟 11.或者,您可以在Device > Management下指定輔助資料介面IP。 即使如此,由於當前的自 註冊方法使用了CLI註冊金鑰過程,這並不是必需的:

FTDv-Azure Cisco Firepower Threat Defense for Azure Device Routing Interfaces Inline Sets DHCP VTEP		
Rules: UTC (UTC+0:00)		
Health	Management	/ 🔍
Status:	Remote Host Address:	NO-IP
Policy: Initial_Health_Policy 2023-06-29 17:28:08	Secondary Address:	
Excluded: None	Status:	•
	Manager Access Interface:	Data Interface
	Manager Access Details:	Configuration

(可選)在管理欄位中為冗餘資料介面指定IP

Objects

步驟 12.部署變更。

Devices

(可選)設定活動/備份介面模式的介面成本:

預設情況下,資料介面上的冗餘管理使用輪詢機制在兩個介面之間分配管理流量。或者,如果某條 WAN鏈路的頻寬比另一條更高,並且您希望該鏈路作為主管理鏈路,而另一條作為備用鏈路,則您 可以將該主鏈路的開銷設定為1,將該備用鏈路的開銷設定為2。在下一個示例中,介面 GigabitEthernet0/0保留為主廣域網鏈路,而GigabitEthernet0/1用作備份管理鏈路:

1. 導航到裝置> FlexConfig連結並建立flexConfig策略。如果已配置並分配給FTD的flexConfig策略 ,請對其進行編輯:

Integration

Device Management	VPN	Troubleshoot
Device Upgrade	Site To Site	File Download
NAT	Remote Access	Threat Defense CLI
QoS	Dynamic Access Policy	Packet Tracer
Platform Settings	Troubleshooting	Packet Capture
FlexConfig	Site to Site Monitoring	
Certificates		

存取FlexConfig功能表

# 2. 建立新的FlexConfig物件:

- 為FlexConfig物件指定名稱。
- 在Deployment和Type部分中分別選擇Everytime和Append。
- 如圖22所示,使用下一個命令設定介面的開銷。
- 按一下Save。

<#root>

interface GigabitEthernet0/0

policy-route cost 1

<=== A cost of 1 means this will be the primary interface for management communication with CDO tenant. interface GigabitEthernet0/1

policy-route cost 2

<=== Cost 2 sets this interface as a backup interface.

CONTRACT Devices / Flexconfig Policy Editor	Analysis Policies Devices	Objects Integra	tion		د•	Return Home	Deploy	۹	0	Ø
MyFlexconfig Enter Description	Add FlexConfig Object	1							0	
Available FlexConfig C FlexConfig Object	InterfaceCost     Description:	2								
User Defined										
V System Defined	A Copy-pasting any rich text might	introduce line break	s while generating CLI. F	lease verify the	CLI before deploy	ment.				
*a Default_DNS_Configure	Invert + 1 Fil Denloum	Europtime		Tune:	Annend				2	
.9 Default_Inspection_Protocol_Disable	insert * an oreproving	everyome		· · · · · · · ·	Appenu			1	3	
* Default_Inspection_Protocol_Enable	interface GigabitEthernet0/0 policy-route cost 1									
*a DHCPv6_Prefx_Delegation_Configure	interface GigabitEthernet0/1	4								
3 DHCPv6_Prefx_Delegation_UnConfigure	policy-route cost 2									
*a DNS_Configure										
.9 DNS_UnConfigure										
Bigrp_Configure										
Bigrp_Interface_Configure										
J Eigrp_UnConfigure										
J Eigrp_Unconfigure_All	▼ Variables									
*a Inspect_IPv6_Configure	Name	Dimension	Default Value	Property (Type:Name)	Override	Description				
_9 Inspect_IPv6_UnConfigure			No records to disp	slay						
*a ISIS_Configure										
*a ISIS_Interface_Configuration										
JISIS_Unconfigure								5		
JISIS_Unconfigure_All									_	
Ta Netflow_Add_Destination						0	ancel	Sav	/e	
-9 Notflow Clear Daramaters							L	_	_	

增加Flexconfig對象

3. 選擇最近建立的物件,並將它新增至如圖所示的「附加彈性組態」區段。儲存更改並部署配置。

Defense Orchestrator Analysis P	olicies Devices	Objects Integration	CReturn Home Deploy	0 0 0	
MyFlexconfig			Migrate Config	Preview Config Sav 4	Cancel
Enter Description				Policy Ace	anments (1)
				Policy Asa	griments (1)
	" a Selected Prep	end FlexConfigs			
Available FlexConfig Object	# Name		Description		
X					
✓ User Defined	2				
TherefaceCost					
✓ System Defined					
B Default_DNS_Configure					
.9 Default_Inspection_Protocol_Disable					
Default_Inspection_Protocol_Enable					
DHCPv6_Prefix_Delegation_Configure					
.9 DHCPv6_Prefix_Delegation_UnConfigure					
DNS_Configure					
.9 DNS_UnConfigure		end FlexConfigs			
Bigrp_Configure	# Name		Description	3	
Bigrp_Interface_Configure	the standard of the			•	0 3
.9 Eigrp_UnConfigure	1 InterfaceCos	st			Ч.
"a Inspect_IPv6_Configure					
Inspect_IPv6_UnConfigure					
"B ISIS_Configure					
"à ISIS_Interface_Configuration					
" ISIS_Unconfigure_All					
Anthony Add Destination					

將物件指派給Flexconfig原則

#### 4. 部署變更。



1. 要驗證,請使用show network命令。形成冗餘管理介面的新例項:

#### > show network

<<----- output omitted for brevity ----->>

-----[ IPv6 ]-----Configuration : Disabled State : Disabled Authentication : Disabled . . . =======[ GigabitEthernet0/0 ]============= State : Enabled Link : Up Name : outside-1 MTU : 1500 MAC Address : 60:45:BD:D8:6F:5C -----[ IPv4 ]------Configuration : Manual Address : 10.6.2.4 Netmask : 255.255.255.0 Gateway : 10.6.3.1 -----[ IPv6 ]-----Configuration : Disabled =======[ GigabitEthernet0/1 ]========== State : Enabled Link : Up Name : outside-2 MTU : 1500 MAC Address : 60:45:BD:D8:67:CA -----[ IPv4 ]------Configuration : Manual Address : 10.6.3.4 Netmask : 255.255.255.0 Gateway : 10.6.3.1 ----- [ IPv6 ]------Configuration : Disabled

2. 該介面現在是sftunnel域的一部分。您可以透過show sftunnel interfaces 和show running-config sftunnel 命令確認這一點:

<#root>

>

show sftunnel interfaces

Physical Interface Name of the Interface GigabitEthernetO/O outside-1 GigabitEthernetO/1 outside-2

>

show running-config sftunnel

```
sftunnel interface outside-2
sftunnel interface outside-1
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

 基於策略的路由將自動拼寫。如果未指定介面開銷,則adaptive-interface選項會設定輪詢處理以 負載平衡兩個介面之間的管理流量:

#### <#root>

>

show running-config route-map

!

```
route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346 permit 5
match ip address FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
set adaptive-interface cost outside-1 outside-2
```

>

```
show access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
```

access-list FMC\_GEN\_056473829\_RBD\_DUAL\_WAN\_ACL\_165748392; 1 elements; name hash: 0x8e8cb508 access-list FMC\_GEN\_056473829\_RBD\_DUAL\_WAN\_ACL\_165748392 line 1 extended permit tcp any any eq 8305 (hi

4. 使用show running-config interface <interface> 命令檢查介面設定:

#### <#root>

>

```
show running-config interface GigabitEthernet 0/0
```

!

interface GigabitEthernet0/0
nameif outside-1
security-level 0
zone-member outside-ecmp
ip address 10.6.2.4 255.255.255.0
policy-route cost 1

>

show running-config interface GigabitEthernet 0/1

!
interface GigabitEthernet0/1
nameif outside-2
security-level 0
zone-member outside-ecmp
ip address 10.6.3.4 255.255.255.0
policy-route cost 2

#### <#root>

#### >

show track

```
Track 1
Response Time Reporter 2 reachability
Reachability is Up
                                      <========= Ensure reachability is up for the monitored interf
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 10
Tracked by:
STATIC-IP-ROUTING 0
Track 2
Response Time Reporter 1 reachability
Reachability is Up
                                      <========== Ensure reachability is up for the monitored interf
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
STATIC-IP-ROUTING 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, BI - BGP InterVRF Gateway of last resort is 10.6.3.1 to network 0.0.00

S\* 0.0.0.0 0.0.0.0 [1/0] via 10.6.3.1, outside-2 [1/0] via 10.6.2.1, outside-1 C 10.6.2.0 255.255.255.0 is directly connected, outside-1 L 10.6.2.4 255.255.255.255 is directly connected, outside-1 C 10.6.3.0 255.255.255.0 is directly connected, outside-2 L 10.6.3.4 255.255.255.255 is directly connected, outside-2

# 相關資訊

- <u>思科技術支援與下載</u>
- 透過Cisco Defense Orchestrator中的雲防火牆管理中心管理防火牆威脅防禦

# 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)。